



HIPAA PRIVACY REGULATIONS EXTRACT OF PREEMPTION REFERENCES

(65 Fed.Reg. 82462 *et seq.* (Dec. 28, 2000))

Prepared by:
Stephen A. Stuart, Senior Staff Counsel
California Office of HIPAA Implementation
January 3, 2003

EXPLANATION

The following document is a tool designed to assist HIPAA-covered persons and entities in analyzing provisions of State law for preemption by the Health Insurance Portability and Accountability Act (HIPAA). The document is an extract of all references to HIPAA preemption of State law set forth in the Final Rule (Standards for Privacy of Individually Identifiable Health Information) issued on December 28, 2000. (65 Fed.Reg. 82462 et seq. (December 28, 2000).)

Please forward any comments, corrections, etc. to the attention of:

Stephen A. Stuart
Senior Staff Counsel
California Office of HIPAA Implementation
1600 Ninth Street, Room 400
Sacramento, CA 95814
(916) 651-6908
sstuart1@ohi.ca.gov

HIPAA Privacy Regulations
Extract of Preemption References
(65 Fed.Reg. 82463 et seq. (Dec. 28, 2000))

I. Background

...

*The Administrative Simplification
Provisions, and Regulatory Actions to
Date*

Part C of title XI consists of sections 1171 through 1179 of the Act. These sections define various terms and impose several requirements on HHS, health plans, health care clearinghouses, and health care providers who conduct the identified transactions electronically. [82470 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

Under section 1178 of the Act, the requirements of part C, as well as any standards or implementation specifications adopted thereunder, preempt contrary state law. There are three exceptions to this general rule of preemption: State laws that the Secretary determines are necessary for certain purposes set forth in the statute; state laws that the Secretary determines address controlled substances; and state laws relating to the privacy of [82470 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] individually identifiable health information that are contrary to and more stringent than the federal requirements. There also are certain areas of state law (generally relating to public health and oversight of health plans) that are explicitly carved out of the general rule of preemption and addressed separately. asking individuals to add social goals into the balance.” [82471 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

Finally, as explained above, section 264 requires the Secretary to issue standards with respect to the privacy of individually identifiable health information. Section 264 also contains a preemption provision that provides that contrary provisions of state laws that are more stringent than the federal standards, requirements, or implementation specifications will not be preempted. [82471 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

1/3/2003

II. Section-by-Section Description of Rule Provisions

...

Part 160—Subpart B—Preemption of State Laws

Statutory Background

Section 1178 of the Act establishes a “general rule” that state law provisions that are contrary to the provisions or requirements of part C of title XI or the standards or implementation specifications adopted or established thereunder are preempted by the federal requirements. The statute provides three exceptions to this general rule: (1) In section 1178(a)(2)(A)(i), for state laws that the Secretary determines are necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery, and other purposes; (2) in section 1178(a)(2)(A)(ii), for state laws that address controlled substances; and (3) in section 1178(a)(2)(B), for state laws relating to the privacy of individually identifiable health information that as provided for by the related provision of section 264(c)(2) of HIPAA, are contrary to and more stringent than the federal requirements. Section 1178 also carves out, in sections 1178(b) and 1178(c), certain areas of state authority that are not limited or invalidated by the provisions of part C of title XI: these areas relate to public health and state regulation of health plans. The NPRM proposed a new Subpart B of the proposed part 160. The new Subpart B, which would apply to all standards, implementation specifications, and requirements adopted under HIPAA, would consist of four sections. Proposed § 160.201 provided that the provisions of Subpart B applied to exception determinations and advisory opinions issued by the Secretary under section 1178. Proposed § 160.202 set out proposed definitions for four terms: (1) “Contrary,” (2) “more stringent,” (3) “relates to the privacy of individually identifiable health information,” and (4) “state law.” The definition of “contrary” was drawn from case law concerning preemption. A seven-part set of specific criteria, drawn from fair information principles, was proposed for the definition of “more stringent.” The definition of “relates to the privacy of individually identifiable health information” was also based on general rule reflecting the statutory general rule and exceptions that generally mirrored the statutory language of the exceptions. The one substantive addition to the statutory exception language was with respect to the statutory exception, “for other purposes.” The following language was added: “for other purposes related to improving the Medicare program, the Medicaid program, or the efficiency and effectiveness of the health care system.” Proposed § 160.204 proposed two processes, one for the making of exception determinations, relating to determinations under section 1178(a)(2)(A) of the Act, the other for the rendering of

1/3/2003

advisory opinions, with respect to section 1178(a)(2)(B) of the Act. The processes proposed were similar in the following respects: (1) Only the state could request an exception determination or advisory opinion, as applicable; (2) both required the request to contain the same information, except that a request for an exception determination also had to set out the length of time the requested exception would be in effect, if less than three years; (3) both sets of requirements provided that requests had to be submitted to the Secretary as required by the Secretary, and until the Secretary's determination was made, the federal standard, requirement or implementation specification remained in effect; (4) both sets of requirements provided that the Secretary's decision would be effective intrastate only; (5) both sets of requirements provided that any change to either the federal or state basis for the Secretary's decision would require a new request, and the federal standard, implementation specification, or requirement would remain in effect until the Secretary acted favorably on the new request; (6) both sets of requirements provided that the Secretary could seek changes to the federal rules or urge states or other organizations to seek changes; and (7) both sets of requirements provided for annual publication of Secretarial decisions. In addition, the process for exception determinations provided for a maximum effective period of three years for such determinations. The following changes have been made to subpart B in the final rules. First, § 160.201 now expressly [82481 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] implements section 1178. Second, the definition of "more stringent" has been changed by eliminating the criterion relating to penalties and by framing the criterion under paragraph (1) more generally. Also, we have clarified that the term "individual" means the person who is the subject of the individually identifiable health information, since the term "individual" is defined this way only in subpart E of part 164, not in part 160. Third, the definition of "state law" has been changed by substituting the words "statute, constitutional provision" for the word "law," the words "common law" for the word "decision," and adding the words "force and" before the word "effect" in the proposed definition. Fourth, in § 160.203, several criteria relating to the statutory grounds for exception determinations have been further spelled out: (1) The words "related to the provision of or payment for health care" have been added to the exception for fraud and abuse; (2) the words "to the extent expressly authorized by statute or regulation" have been added to the exception for state regulation of health plans; (3) the words "of serving a compelling need related to public health, safety, or welfare, and, where a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, where the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served" have been added to the general exception "for other purposes"; and (4) the statutory provision regarding controlled substances has been elaborated on as follows: "Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substance, as defined at 21 U.S.C. 802, or which is deemed a controlled substance by state law." The most extensive changes have been made to proposed § 160.204. The provision for advisory

1/3/2003

opinions has been eliminated. Section 160.204 now sets out only a process for requesting exception determinations. In most respects, this process is the same as proposed. However, the proposed restriction of the effect of exception determinations to wholly intrastate transactions has been eliminated. Section 160.204(a) has been modified to allow any person, not just a state, to submit a request for an exception determination, and clarifies that requests from states may be made by the state's chief elected official or his or her designee. Proposed § 160.204(a)(3) stated that if it is determined that the federal standard, requirement, or implementation specification in question meets the exception criteria as well as or better than the state law for which the exception is requested, the request will be denied; this language has been deleted. Thus, the criterion for granting or denying an exception request is whether the applicable exception criterion or criteria are met. A new § 160.205 is also adopted, replacing part of what was proposed at proposed § 160.204. The new § 160.205 sets out the rules relating to the effectiveness of exception determinations. Exception determinations are effective until either the underlying federal or state laws change or the exception is revoked, by the Secretary, based on a determination that the grounds supporting the exception no longer exist. The proposed maximum of three years has been eliminated.

Relationship to Other Federal Laws

Covered entities subject to these rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act. Thus, covered entities will need to determine how the privacy regulation will affect their ability to comply with these other federal laws. Many commenters raised questions about how different federal statutes and regulations intersect with the privacy regulation. While we address specific concerns in the response to comments later in the preamble, in this section, we explore some of the general interaction issues. These summaries do not identify all possible conflicts or overlaps of the privacy regulation and other federal laws, but should provide general guidance for complying with both the privacy regulation and other federal laws. The summaries also provide examples of how covered entities can analyze other federal laws when specific questions arise. HHS may consult with other agencies concerning the interpretation of other federal laws as necessary.

Implied Repeal Analysis

When faced with the need to determine how different federal laws interact with one another, we turn to the judiciary's approach. Courts apply the implied repeal analysis

1/3/2003

to resolve tensions that appear to exist between two or more statutes. While the implication of a regulation-on regulation conflict is unclear, courts agree that administrative rules and regulations that do not conflict with express statutory provisions have the force and effect of law. Thus, we believe courts would apply the standard rules of interpretation that apply to statutes to address questions of interpretation with regard to regulatory conflicts. When faced with two potentially conflicting statutes, courts attempt to construe them so that both are given effect. If this construction is not possible, courts will look for express language in the later statute, or an intent in its legislative history, indicating that Congress intended the later statute to repeal the earlier one. If there is no expressed intent to repeal the earlier statute, courts will characterize the statutes as either general or specific. Ordinarily, later, general statutes will not repeal the special provisions of an earlier, specific statute. In some cases, when a later, general statute creates an irreconcilable conflict or is manifestly inconsistent with the earlier, specific statute in a manner that indicates a clear and manifest Congressional intent to repeal the earlier statute, courts will find that the later statute repeals the earlier statute by implication. In these cases, the latest legislative action may prevail and repeal the prior law, but only to the extent of the conflict. There should be few instances in which conflicts exist between a statute or regulation and the rules below. For example, if a statute permits a covered entity to disclose protected health information and the rules below permit such a disclosure, no conflict arises; the covered entity could comply with both and choose whether or not to disclose the information. In instances in which a potential conflict appears, we would attempt to resolve it so that both laws applied. For example, if a statute or regulation permits dissemination of protected health information, but the rules below prohibit the use or disclosure without an authorization, we believe a covered entity would be able to comply with both because it could obtain an authorization under § 164.508 before disseminating the information under the other law. Many apparent conflicts will not be true conflicts. For example, if a conflict [82482 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] appears to exist because a previous statute or regulation requires a specific use or disclosure of protected health information that the rules below appear to prohibit, the use or disclosure pursuant to that statute or regulation would not be a violation of the privacy regulation because § 164.512(a) permits covered entities to use or disclose protected health information as required by law. If a statute or regulation prohibits dissemination of protected health information, but the privacy regulation requires that an individual have access to that information, the earlier, more specific statute would apply. The interaction between the Clinical Laboratory Improvement Amendments regulation is an example of this type of conflict. From our review of several federal laws, it appears that Congress did not intend for the privacy regulation to overrule existing statutory requirements in these instances.

Examples of Interaction

1/3/2003

We have summarized how certain federal laws interact with the privacy regulation to provide specific guidance in areas deserving special attention and to serve as examples of the analysis involved. In the Response to Comment section, we have provided our responses to specific questions raised during the comment period.

The Privacy Act

The Privacy Act of 1974, 5 U.S.C. 552a, prohibits disclosures of records contained in a system of records maintained by a federal agency (or its contractors) without the written request or consent of the individual to whom the record pertains. This general rule is subject to various statutory exceptions. In addition to the disclosures explicitly permitted in the statute, the Privacy Act permits agencies to disclose information for other purposes compatible with the purpose for which the information was collected by identifying the disclosure as a “routine use” and publishing notice of it in the Federal Register. The Act applies to all federal agencies and certain federal contractors who operate Privacy Act systems of records on behalf of federal agencies. Some federal agencies and contractors of federal agencies that are covered entities under the privacy rules are subject to the Privacy Act. These entities must comply with all applicable federal statutes and regulations. For example, if the privacy regulation permits a disclosure, but the disclosure is not permitted under the Privacy Act, the federal agency may not make the disclosure. If, however, the Privacy Act allows a federal agency the discretion to make a routine use disclosure, but the privacy regulation prohibits the disclosure, the federal agency will have to apply its discretion in a way that complies with the regulation. This means not making the particular disclosure.

The Freedom of Information Act

FOIA, 5 U.S.C. 552, provides for public disclosure, upon the request of any person, of many types of information in the possession of the federal government, subject to nine exemptions and three exclusions. For example, Exemption 6 permits federal agencies to withhold “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. 552(b)(6). Uses and disclosures required by FOIA come within § 164.512(a) of the privacy regulation that permits uses or disclosures required by law if the uses or disclosures meet the relevant requirements of the law. Thus, a federal agency must determine whether it may apply an exemption or exclusion to redact the protected health information when responding to a FOIA request. When a FOIA request asks for documents that include protected health information, we believe the agency, when appropriate, must apply Exemption 6 to preclude the release of medical files or otherwise redact identifying details before disclosing the remaining information. We offer the following analysis for federal agencies and federal contractors who operate Privacy Act systems of records on behalf of federal agencies and must comply with FOIA and the privacy regulation. If presented with a FOIA request that would result

1/3/2003

in the disclosure of protected health information, a federal agency must first determine if FOIA requires the disclosure or if an exemption or exclusion would be appropriate. We believe that generally a disclosure of protected health information, when requested under FOIA, would come within FOIA Exemption 6. We recognize, however, that the application of this exemption to information about deceased individuals requires a different analysis than that applicable to living individuals because, as a general rule, under the Privacy Act, privacy rights are extinguished at death. However, under FOIA, it is entirely appropriate to consider the privacy interests of a decedent's survivors under Exemption 6. See Department of Justice FOIA Guide 2000, Exemption 6: Privacy Considerations. Covered entities subject to FOIA must evaluate each disclosure on a case-by-case basis, as they do now under current FOIA procedures.

*Federal Substance Abuse
Confidentiality Requirements*

The federal confidentiality of substance abuse patient records statute, section 543 of the Public Health Service Act, 42 U.S.C. 290dd-2, and its implementing regulation, 42 CFR part 2, establish confidentiality requirements for patient records that are maintained in connection with the performance of any federally-assisted specialized alcohol or drug abuse program. Substance abuse programs are generally programs or personnel that provide alcohol or drug abuse treatment, diagnosis, or referral for treatment. The term "federally-assisted" is broadly defined and includes federally conducted or funded programs, federally licensed or certified programs, and programs that are tax exempt. Certain exceptions apply to information held by the Veterans Administration and the Armed Forces. There are a number of health care providers that are subject to both these rules and the substance abuse statute and regulations. In most cases, a conflict will not exist between these rules. These privacy rules permit a health care provider to disclose information in a number of situations that are not permitted under the substance abuse regulation. For example, disclosures allowed, without patient authorization, under the privacy rule for law enforcement, judicial and administrative proceedings, public health, health oversight, directory assistance, and as required by other laws would generally be prohibited under the substance abuse statute and regulation. However, because these disclosures are permissive and not mandatory, there is no conflict. An entity would not be in violation of the privacy rules for failing to make these disclosures. Similarly, provisions in the substance abuse regulation provide for permissive disclosures in case of medical emergencies, to the FDA, for research activities, for audit and evaluation activities, and in response to certain court orders. Because these are permissive disclosures, programs subject to both the privacy rules and the substance abuse rule are able to comply with both rules even if the privacy rules restrict these types of disclosures. In addition, the privacy rules generally require that an individual be given access to his or her own health information. Under the substance abuse [82483 Federal Register / Vol. 65, No. 250 / Thursday, December

1/3/2003

28, 2000 / Rules and Regulations] regulation, programs may provide such access, so there is no conflict. The substance abuse regulation requires notice to patients of the substance abuse confidentiality requirements and provides for written consent for disclosure. While the privacy rules have requirements that are somewhat different, the program may use notice and authorization forms that include all the elements required by both regulations. The substance abuse rule provides a sample notice and a sample authorization form and states that the use of these forms would be sufficient. While these forms do not satisfy all of the requirements of the privacy regulation, there is no conflict because the substance abuse regulation does not mandate the use of these forms.

Employee Retirement Income Security Act of 1974

ERISA was enacted in 1974 to regulate pension and welfare employee benefit plans established by private sector employers, unions, or both, to provide benefits to their workers and dependents. Under ERISA, plans that provide “through the purchase of insurance or otherwise * * * medical, surgical, or hospital care or benefits, or benefits in the event of sickness, accident, disability, [or] death” are defined as employee welfare benefit plans. 29 U.S.C. 1002(1). In 1996, HIPAA amended ERISA to require portability, nondiscrimination, and renewability of health benefits provided by group health plans and group health insurance issuers. Numerous, although not all, ERISA plans are covered under the rules proposed below as “health plans.” Section 514(a) of ERISA, 29 U.S.C. 1144(a), preempts all state laws that “relate to” any employee benefit plan. However, section 514(b) of ERISA, 29 U.S.C. 1144(b)(2)(A), expressly saves from preemption state laws that regulate insurance. Section 514(b)(2)(B) of ERISA, 29 U.S.C. 1144(b)(2)(B), provides that an ERISA plan is deemed not to be an insurer for the purpose of regulating the plan under the state insurance laws. Thus, under the deemer clause, states may not treat ERISA plans as insurers subject to direct regulation by state law. Finally, section 514(d) of ERISA, 29 U.S.C. 1144(d), provides that ERISA does not “alter, amend, modify, invalidate, impair, or supersede any law of the United States.” We considered whether the preemption provision of section 264(c)(2) of HIPAA would give effect to state laws that would otherwise be preempted by section 514(a) of ERISA. As discussed above, our reading of the statutes together is that the effect of section 264(c)(2) is only to leave in place state privacy protections that would otherwise apply and that are more stringent than the federal privacy protections. Many health plans covered by the privacy regulation are also subject to ERISA requirements. Our discussions and consultations have not uncovered any particular ERISA requirements that would conflict with the rules.

The Family Educational Rights and Privacy Act

1/3/2003

FERPA, as amended, 20 U.S.C. 1232g, provides parents of students and eligible students (students who are 18 or older) with privacy protections and rights for the records of students maintained by federally funded educational agencies or institutions or persons acting for these agencies or institutions. We have excluded education records covered by FERPA, including those education records designated as education records under Parts B, C, and D of the Individuals with Disabilities Education Act Amendments of 1997, from the definition of protected health information. For example, individually identifiable health information of students under the age of 18 created by a nurse in a primary or secondary school that receives federal funds and that is subject to FERPA is an education record, but not protected health information. Therefore, the privacy regulation does not apply. We followed this course because Congress specifically addressed how information in education records should be protected in FERPA. We have also excluded certain records, those described at 20 U.S.C. 1232g(a)(4)(B)(iv), from the definition of protected health information because FERPA also provided a specific structure for the maintenance of these records. These are records (1) of students who are 18 years or older or are attending post-secondary educational institutions, (2) maintained by a physician, psychiatrist, psychologist, or recognized professional or paraprofessional acting or assisting in that capacity, (3) that are made, maintained, or used only in connection with the provision of treatment to the student, and (4) that are not available to anyone, except a physician or appropriate professional reviewing the record as designated by the student. Because FERPA excludes these records from its protections only to the extent they are not available to anyone other than persons providing treatment to students, any use or disclosure of the record for other purposes, including providing access to the individual student who is the subject of the information, would turn the record into an education record. As education records, they would be subject to the protections of FERPA. These exclusions are not applicable to all schools, however. If a school does not receive federal funds, it is not an educational agency or institution as defined by FERPA. Therefore, its records that contain individually identifiable health information are not education records. These records may be protected health information. The educational institution or agency that employs a school nurse is subject to our regulation as a health care provider if the school nurse or the school engages in a HIPAA transaction. While we strongly believe every individual should have the same level of privacy protection for his/her individually identifiable health information, Congress did not provide us with authority to disturb the scheme it had devised for records maintained by educational institutions and agencies under FERPA. We do not believe Congress intended to amend or preempt FERPA when it enacted HIPAA. With regard to the records described at 20 U.S.C. 1232g(a)(4)(b)(iv), we considered requiring health care providers engaged in HIPAA transactions to comply with the privacy regulation up to the point these records were used or disclosed for purposes other than treatment. At that point, the records would be converted from protected health information into education records. This conversion would occur any time a student sought to exercise his/her access rights. The provider, then, would need to treat the record in

1/3/2003

accordance with FERPA's requirements and be relieved from its obligations under the privacy regulation. We chose not to adopt this approach because it would be unduly burdensome to require providers to comply with two different, yet similar, sets of regulations and inconsistent with the policy in FERPA that these records be exempt from regulation to the extent the records were used only to treat the student.

Gramm-Leach-Bliley

In 1999, Congress passed Gramm- Leach-Bliley (GLB), Pub. L. 106–102, which included provisions, section 501 et seq., that limit the ability of financial institutions to disclose “nonpublic personal information” about consumers to non-affiliated third parties and require financial institutions to provide customers with their privacy policies and practices with respect to nonpublic [82484 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] personal information. In addition, Congress required seven agencies with jurisdiction over financial institutions to promulgate regulations as necessary to implement these provisions. GLB and its accompanying regulations define “financial institutions” as including institutions engaged in the financial activities of bank holding companies, which may include the business of insuring. See 15 U.S.C. 6809(3); 12 U.S.C. 1843(k). However, Congress did not provide the designated federal agencies with the authority to regulate health insurers. Instead, it provided states with an incentive to adopt and have their state insurance authorities enforce these rules. See 15 U.S.C. 6805. If a state were to adopt laws consistent with GLB, health insurers would have to determine how to comply with both sets of rules. Thus, GLB has caused concern and confusion among health plans that are subject to our privacy regulation. Although Congress remained silent as to its understanding of the interaction of GLB and HIPAA's privacy provisions, the Federal Trade Commission and other agencies implementing the GLB privacy provisions noted in the preamble to their GLB regulations that they “would consult with HHS to avoid the imposition of duplicative or inconsistent requirements.” 65 Fed. Reg. 33646, 33648 (2000). Additionally, the FTC also noted that “persons engaged in providing insurance” would be within the enforcement jurisdiction of state insurance authorities and not within the jurisdiction of the FTC. Id. Because the FTC has clearly stated that it will not enforce the GLB privacy provisions against persons engaged in providing insurance, health plans will not be subject to dual federal agency jurisdiction for information that is both nonpublic personal information and protected health information. If states choose to adopt GLB-like laws or regulations, which may or may not track the federal rules completely, health plans would need to evaluate these laws under the preemption analysis described in subpart B of Part 160.

Federally Funded Health Programs

These rules will affect various federal programs, some of which may have requirements that are, or appear to be, inconsistent with the requirements of these

1/3/2003

regulations. These programs include those operated directly by the federal government (such as health programs for military personnel and veterans) as well as programs in which health services or benefits are provided by the private sector or by state or local governments, but which are governed by various federal laws (such as Medicare, Medicaid, and ERISA). Congress explicitly included some of these programs in HIPAA, subjecting them directly to the privacy regulation. Section 1171 of the Act defines the term “health plan” to include the following federally conducted, regulated, or funded programs: Group plans under ERISA that either have 50 or more participants or are administered by an entity other than the employer who established and maintains the plan; federally qualified health maintenance organizations; Medicare; Medicaid; Medicare supplemental policies; the health care program for active military personnel; the health care program for veterans; the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS); the Indian health service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, *et seq.*; and the Federal Employees Health Benefits Program. There also are many other federally conducted, regulated, or funded programs in which individually identifiable health information is created or maintained, but which do not come within the statutory definition of “health plan.” While these latter types of federally conducted, regulated, or assisted programs are not explicitly covered by part C of title XI in the same way that the programs listed in the statutory definition of “health plan” are covered, the statute may nonetheless apply to transactions and other activities conducted under such programs. This is likely to be the case when the federal entity or federally regulated or funded entity provides health services; the requirements of part C may apply to such an entity as a “health care provider.” Thus, the issue of how different federal requirements apply is likely to arise in numerous contexts. There are a number of authorities under the Public Health Service Act and other legislation that contain explicit confidentiality requirements, either in the enabling legislation or in the implementing regulations. Many of these are so general that there would appear to be no problem of inconsistency, in that nothing in those laws or regulations would appear to restrict the provider’s ability to comply with the privacy regulation’s requirements. There may, however, be authorities under which either the requirements of the enabling legislation or of the program regulations would impose requirements that differ from these rules. For example, regulations applicable to the substance abuse block grant program funded under section 1943(b) of the Public Health Service Act require compliance with 42 CFR part 2, and, thus, raise the issues identified above in the substance abuse confidentiality regulations discussion. There are a number of federal programs which, either by statute or by regulation, restrict the disclosure of patient information to, with minor exceptions, disclosures “required by law.” See, for example, the program of projects for prevention and control of sexually transmitted diseases funded under section 318(e)(5) of the Public Health Service Act (42 CFR 51b.404); the regulations implementing the community health center program funded under section 330 of the Public Health Service Act (42 CFR 51c.110); the regulations implementing the program of grants for family planning services under title X of the

1/3/2003

Public Health Service Act (42 CFR 59.15); the regulations implementing the program of grants for black lung clinics funded under 30 U.S.C. 437(a) (42 CFR 55a.104); the regulations implementing the program of maternal and child health projects funded under section 501 of the Act (42 CFR 51a.6); the regulations implementing the program of medical examinations of coal miners (42 CFR 37.80(a)). These legal requirements would restrict the grantees or other entities providing services under the programs involved from making many of the disclosures that §§ 164.510 or 164.512 would permit. In some cases, permissive disclosures for treatment, payment, or health care operations would also be limited. Because §§ 164.510 and 164.512 are merely permissive, there would not be a conflict between the program requirements, because it would be possible to comply with both. However, entities subject to both sets of requirements would not have the total range of discretion that they would have if they were subject only to this regulation.

Food, Drug, and Cosmetic Act

The Food, Drug, and Cosmetic Act, 21 U.S.C. 301, et seq., and its accompanying regulations outline the responsibilities of the Food and Drug Administration with regard to monitoring the safety and effectiveness of drugs and devices. Part of the agency's responsibility is to obtain reports about adverse events, track medical devices, and engage in other types of post marketing surveillance. Because many of these reports contain protected health information, the information within them may come within the purview of the privacy rules. [82485 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] Although some of these reports are required by the Food, Drug, and Cosmetic Act or its accompanying regulations, other types of reporting are voluntary. We believe that these reports, while not mandated, play a critical role in ensuring that individuals receive safe and effective drugs and devices. Therefore, in § 164.512(b)(1)(iii), we have provided that covered entities may disclose protected health information to a person subject to the jurisdiction of the Food and Drug Administration for specified purposes, such as reporting adverse events, tracking medical devices, or engaging in other post marketing surveillance. We describe the scope and conditions of such disclosures in more detail in § 164.512(b).

Clinical Laboratory Improvement Amendments

CLIA, 42 U.S.C. 263a, and the accompanying regulations, 42 CFR part 493, require clinical laboratories to comply with standards regarding the testing of human specimens. This law requires clinical laboratories to disclose test results or reports only to authorized persons, as defined by state law. If a state does not define the term, the federal law defines it as the person who orders the test. We realize that the person ordering the test is most likely a health care provider and not the individual who is the subject of the protected health information included within the result or

1/3/2003

report. Under this requirement, therefore, a clinical laboratory may be prohibited by law from providing the individual who is the subject of the test result or report with access to this information. Although we believe individuals should be able to have access to their individually identifiable health information, we recognize that in the specific area of clinical laboratory testing and reporting, the Health Care Financing Administration, through regulation, has provided that access may be more limited. To accommodate this requirement, we have provided at § 164.524(1)(iii) that covered entities maintaining protected health information that is subject to the CLIA requirements do not have to provide individuals with a right of access to or a right to inspect and obtain a copy of this information if the disclosure of the information to the individual would be prohibited by CLIA. Not all clinical laboratories, however, will be exempted from providing individuals with these rights. If a clinical laboratory operates in a state in which the term “authorized person” is defined to include the individual, the clinical laboratory would have to provide the individual with these rights. Similarly, if the individual was the person who ordered the test and an authorized person included such a person, the laboratory would be required to provide the individual with these rights. Additionally, CLIA regulations exempt the components or functions of “research laboratories that test human specimens but do not report patient specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients” from the CLIA regulatory scheme. 42 CFR 493.3(a)(2). If subject to the access requirements of this regulation, such entities would be forced to meet the requirements of CLIA from which they are currently exempt. To eliminate this additional regulatory burden, we have also excluded covered entities that are exempt from CLIA under that rule from the access requirement of this regulation. Although we are concerned about the lack of immediate access by the individual, we believe that, in most cases, individuals who receive clinical tests will be able to receive their test results or reports through the health care provider who ordered the test for them. The provider will receive the information from the clinical laboratory. Assuming that the provider is a covered entity, the individual will have the right of access and right to inspect and copy this protected health information through his or her provider.

Other Mandatory Federal or State Laws

Many federal laws require covered entities to provide specific information to specific entities in specific circumstances. If a federal law requires a covered entity to disclose a specific type of information, the covered entity would not need an authorization under § 164.508 to make the disclosure because the final rule permits covered entities to make disclosures that are required by law under § 164.512(a). Other laws, such as the Social Security Act (including its Medicare and Medicaid provisions), the Family and Medical Leave Act, the Public Health Service Act, Department of Transportation regulations, the Environmental Protection Act and its accompanying regulations, the National Labor Relations Act, the Federal Aviation

1/3/2003

Administration, and the Federal Highway Administration rules, may also contain provisions that require covered entities or others to use or disclose protected health information for specific purposes. When a covered entity is faced with a question as to whether the privacy regulation would prohibit the disclosure of protected health information that it seeks to disclose pursuant to a federal law, the covered entity should determine if the disclosure is required by that law. In other words, it must determine if the disclosure is mandatory rather than merely permissible. If it is mandatory, a covered entity may disclose the protected health information pursuant to § 164.512(a), which permits covered entities to disclose protected health information without an authorization when the disclosure is required by law. If the disclosure is not required (but only permitted) by the federal law, the covered entity must determine if the disclosure comes within one of the other permissible disclosures. If the disclosure does not come within one of the provisions for permissible disclosures, the covered entity must obtain an authorization from the individual who is the subject of the information or de-identify the information before disclosing it. If another federal law prohibits a covered entity from using or disclosing information that is also protected health information, but the privacy regulation permits the use or disclosure, a covered entity will need to comply with the other federal law and not use or disclose the information.

Federal Disability Nondiscrimination Laws

The federal laws barring discrimination on the basis of disability protect the confidentiality of certain medical information. The information protected by these laws falls within the larger definition of “health information” under this privacy regulation. The two primary disability nondiscrimination laws are the Americans with Disabilities Act (ADA), 42 U.S.C. 12101 et seq., and the Rehabilitation Act of 1973, as amended, 29 U.S.C. 701 et seq., although other laws barring discrimination on the basis of disability (such as the nondiscrimination provisions of the Workforce Investment Act of 1988, 29 U.S.C. 2938) may also apply. Federal disability nondiscrimination laws cover two general categories of entities relevant to this discussion: employers and entities that receive federal financial assistance. Employers are not covered entities under the privacy regulation. Many employers, however, are subject to the federal disability nondiscrimination laws and, therefore, must protect the [82486 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] 1 The Principles are: (1) Notice; (2) Choice (i.e., consent); (3) Onward Transfer (i.e., subsequent disclosures); (4) Security; (5) Data Integrity; (6) Access; and (7) Enforcement. Department of Commerce, Safe Harbor Principles, July 21, 2000 (“Principles”). They do not apply to manually processed data. confidentiality of all medical information concerning their applicants and employees. The employment provisions of the ADA, 42 U.S.C. 12111 et seq., expressly cover employers of 15 or more employees, employment agencies, labor organizations, and joint labor management committees. Since 1992, employment

1/3/2003

discrimination complaints arising under sections 501, 503, and 504 of the Rehabilitation Act also have been subject to the ADA's employment nondiscrimination standards. See "Rehabilitation Act Amendments," Pub. L. No. 102-569, 106 Stat. 4344. Employers subject to ADA nondiscrimination standards have confidentiality obligations regarding applicant and employee medical information. Employers must treat such medical information, including medical information from voluntary health or wellness programs and any medical information that is voluntarily disclosed as a confidential medical record, subject to limited exceptions. Transmission of health information by an employer to a covered entity, such as a group health plan, is governed by the ADA confidentiality restrictions. The ADA, however, has been interpreted to permit an employer to use medical information for insurance purposes. See 29 CFR part 1630 App. at § 1630.14(b) (describing such use with reference to 29 CFR 1630.16(f), which in turn explains that the ADA regulation "is not intended to disrupt the current regulatory structure for self-insured employers * * * or current industry practices in sales, underwriting, pricing, administrative and other services, claims and similar insurance related activities based on classification of risks as regulated by the states"). See also, "Enforcement Guidance on Disability-Related Inquiries and Medical Examinations of Employees under the Americans with Disabilities Act," 4, n.10 (July 26, 2000), II FEP Manual (BNA) II ("Enforcement Guidance on Employees"). See generally, "ADA Enforcement Guidance on Preemployment Disability-Related Questions and Medical Examinations" (October 10, 1995), 8 FEP Manual (BNA) 405:7191 (1995) (also available at <http://www.eeoc.gov>). Thus, use of medical information for insurance purposes may include transmission of health information to a covered entity. If an employer-sponsored group health plan is closely linked to an employer, the group health plan may be subject to ADA confidentiality restrictions, as well as this privacy regulation. See *Carparts Distribution Center, Inc. v. Automotive Wholesaler's Association of New England, Inc.*, 37 F.3d 12 (1st Cir. 1994)(setting forth three bases for ADA Title I jurisdiction over an employer-provided medical reimbursement plan, in a discrimination challenge to the plan's HIV/AIDS cap). Transmission of applicant or employee health information by the employer's management to the group health plan may be permitted under the ADA standards as the use of medical information for insurance purposes. Similarly, disclosure of such medical information by the group health plan, under the limited circumstances permitted by this privacy regulation, may involve use of the information for insurance purposes as broadly described in the ADA discussion above. Entities that receive federal financial assistance, which may also be covered entities under the privacy regulation, are subject to section 504 of the Rehabilitation Act (29 U.S.C. 794) and its implementing regulations. Each federal agency has promulgated such regulations that apply to entities that receive financial assistance from that agency ("recipients"). These regulations may limit the disclosure of medical information about persons who apply to or participate in a federal financially assisted program or activity. For example, the Department of Labor's section 504 regulation (found at 29 CFR part 32), consistent with the ADA standards, requires recipients that conduct employment-related

1/3/2003

programs, including employment training programs, to maintain confidentiality regarding any information about the medical condition or history of applicants to or participants in the program or activity. Such information must be kept separate from other information about the applicant or participant and may be provided to certain specified individuals and entities, but only under certain limited circumstances described in the regulation. See 29 CFR 32.15(d). Apart from those circumstances, the information must be afforded the same confidential treatment as medical records, *id.* Also, recipients of federal financial assistance from the Department of Health and Human Services, such as hospitals, are subject to the ADA's employment nondiscrimination standards. They must, accordingly, maintain confidentiality regarding the medical condition or history of applicants for employment and employees. The statutes and implementing regulations under which the federal financial assistance is provided may contain additional provisions regulating collection and disclosure of medical, health, and disability-related information. See, e.g., section 188 of the Workforce Investment Act of 1988 (29 U.S.C. 2938) and 29 CFR 37.3(b). Thus, covered entities that are subject to this privacy regulation, may also be subject to the restrictions in these laws as well.

*U.S. Safe Harbor Privacy Principles
(European Union Directive on Data
Protection)*

The E.U. Directive became effective in October 1998 and prohibits European Union Countries from permitting the transfer of personal data to another country without ensuring that an "adequate level of protection," as determined by the European Commission, exists in the other country or pursuant to one of the Directive's derogations of this rule, such as pursuant to unambiguous consent or to fulfill a contract with the individual. In July 2000, the European Commission concluded that the U.S. Safe Harbor Privacy Principles 1 constituted "adequate protection." Adherence to the Principles is voluntary. Organizations wishing to engage in the exchange of personal data with E.U. countries may assert compliance with the Principles as one means of obtaining data from E.U. countries. The Department of Commerce, which negotiated these Principles with the European Commission, has provided guidance for U.S. organizations seeking to adhere to the guidelines and comply with U.S. law. We believe this guidance addresses the concerns covered entities seeking to transfer personal data from E.U. countries may have. When "U.S. law imposes a conflicting obligation, U.S. organizations whether in the safe harbor or not must comply with the law." An organization does not need to comply with the Principles if a conflicting U.S. law "explicitly authorizes" the particular conduct. The organization's non-compliance is "limited to the extent necessary to meet the overriding legitimate interests further[ed] by such authorization." However, if only a difference exists such that an "option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible." Questions regarding compliance and interpretation will be decided based on U.S.

1/3/2003

law. See Department of Commerce, Memorandum on Damages for Breaches [82487 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law 5 (July 17, 2000); Department of Commerce, Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000, 65 FR 45666 (2000). The Principles and our privacy regulation are based on common principles of fair information practices. We believe they are essentially consistent and that an organization complying with our privacy regulation can fairly and correctly self-certify that it complies with the Principles. If a true conflict arises between the privacy regulation and the Principles, the Department of Commerce's guidance provides that an entity must comply with the U.S. law.

Part 164—Subpart E—Privacy

...

Section 164.502—General Rules for Uses and Disclosures of Protected Health Information

...

Section 164.502(g)—Personal Representatives

...

Under this provision, we do not provide a minor with the authority to act under the rule unless the state has given them the ability to obtain health care without consent of a parent, or the parent has assented. In addition, we defer to state law where the state authorizes or prohibits disclosure of protected health information to a parent. See part 160, subpart B, Preemption of State Law. [82500 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

Section 164.506—Uses and Disclosures for Treatment, Payment, and Health Care Operations

...

Effect of Consent

1/3/2003

These consents, as well as the authorizations described in § 164.508, should not be construed to waive, directly or indirectly, any privilege granted under federal, state, or local law or procedure. Consents obtained under this regulation are not appropriate for the disposition of more technical and legal proceedings and may not comport with procedures and standards of federal, state, or local judicial practice. For example, state courts and other decision-making bodies may choose to examine more closely the circumstances and propriety of such consent and may adopt more protective standards for application in their proceedings. In the judicial setting, as in the legislative and executive settings, states may provide for greater protection of privacy. Additionally, both the Congress and the Secretary have established a general approach to protecting from explicit preemption state laws that are more protective of privacy than the protections set forth in this regulation. [82513 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

**Section 164.510—Uses and Disclosures
Requiring an Opportunity for the
Individual To Agree or To Object**

...

*Section 164.512(c)—Disclosures About
Victims of Abuse, Neglect or Domestic
Violence*

The NPRM included two provisions related to disclosures about persons who are victims of abuse. In the NPRM, we would have allowed covered entities to report child abuse to a public health authority or other appropriate authority authorized by law to receive reports of child abuse or neglect. In addition, under proposed § 164.510(f)(3) of the NPRM, we would have allowed covered entities to disclose protected health information about a victim of a crime, abuse or other harm to a law enforcement official under certain circumstances. The NPRM recognized that most, if not all, states had laws that mandated reporting of child abuse or neglect to the appropriate authorities. Moreover, HIPAA expressly carved out state laws on child abuse and neglect from preemption or any other interference. The NPRM further acknowledged that most, but not all, states had laws mandating the reporting of abuse, neglect or exploitation of the elderly or other vulnerable adults. We did not intend to impede reporting in compliance with these laws. [82527 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

Section 164.512(f)—Disclosure for Law

1/3/2003

Enforcement Purposes

...

Additional Considerations

Under the NPRM and under the final rule, to obtain protected health information, law enforcement officials must comply with whatever other law is applicable. In certain circumstances, while this provision could authorize a covered entity to disclose protected health information to law enforcement officials, there could be additional applicable statutes or rules that further govern the specific disclosure. If the preemption provisions of this regulation do not apply, the covered entity must comply with the requirements or limitations established by such other law, regulation or judicial precedent. See §§ 160.201 through 160.205. For example, if state law permits disclosure only after compulsory process with court review, a provider or payor is not allowed to disclose information to state law enforcement officials unless the officials have complied with that requirement. [82533 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

...

III. Section-by-Section Discussion of Comments

General Comments

...

Comments on the Need for Privacy Standards, and Effects of this Regulation on Current Protections

...

Comment: Many commenters expressed concerns that this regulation will allow access to health information by those who today do not have such access, or would allow their physician to disclose information which may not lawfully be disclosed today. Many of these commenters stated that today, they consent to every disclosure of health information about them, and that absent their consent the privacy of their health information is “absolute.” Others stated that, today, health information is disclosed only pursuant to a judicial order. Several commenters were concerned that this regulation would override stronger state privacy protection.

Response: This regulation does not, and cannot, reduce current privacy protections. The statutory language of the HIPAA specifically mandates that this regulation does not preempt state laws that are more protective of privacy. As discussed in more

1/3/2003

detail in later this preamble, while many people believe that they must be asked permission prior to any release of health information about them, current laws generally do not impose such a requirement. Similarly, as discussed in more detail later in this preamble, judicial review is required today only for a small proportion of releases of health information.

...

Part 160—Subpart B—Preemption of State Law

We summarize and respond below to comments received in the Transactions rulemaking on the issue of preemption, as well as those received on this topic in the Privacy rulemaking. Because no process was proposed in the Transactions rulemaking for granting exceptions under section 1178(a)(2)(A), a process for making exception determinations was not adopted in the Transactions Rule. Instead, since a process for making exception determinations was proposed in the Privacy rulemaking, we decided that the comments received in the Transactions rulemaking should be considered and addressed in conjunction with the comments received on the process proposed in the Privacy rulemaking. See 65 FR 50318 for a fuller discussion. Accordingly, we discuss the preemption comments received in the Transactions rulemaking where relevant below.

Comment: The majority of comments on preemption addressed the subject in general terms. Numerous comments, particularly from plans and providers, argued that the proposed preemption provisions were burdensome, ineffective, or insufficient, and that complete federal preemption of the “patchwork” of state privacy laws is needed. They also argued that the proposed preemption provisions are likely to invite litigation. Various practical arguments in support of this position were made. Some of these comments recognized that the Secretary’s authority under section 1178 of the Act is limited and acknowledged that the Secretary’s proposals were within her statutory authority. One commenter suggested that the exception determination process would result in a very costly and laborious and sometimes inconsistent analysis of the occasions in which state law would [82580 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] survive federal preemption, and thus suggested the final privacy regulations preempt state law with only limited exceptions, such as reporting child abuse. Many other comments, however, recommended changing the proposed preemption provisions to preempt state privacy laws on as blanket a basis as possible. One comment argued that the assumption that more stringent privacy laws are better is not necessarily true, citing a 1999 GAO report finding evidence that the stringent state confidentiality laws of Minnesota halted the collection of comparative information on health care quality. Several comments in this vein were also received in the Transactions rulemaking. The majority of these comments took the position that exceptions to the federal standards should either be prohibited or discouraged.

1/3/2003

It was argued that granting exceptions to the standards, particularly the transactions standards, would be inconsistent with the statute's objective of promoting administrative simplification through the use of uniform transactions. Many other commenters, however, endorsed the "federal floor" approach of the proposed rules. (These comments were made in the context of the proposed privacy regulations.) These comments argued that this approach was preferable because it would not impair the effectiveness of state privacy laws that are more protective of privacy, while raising the protection afforded medical information in states that do not enact laws that are as protective as the rules below. Some comments argued, however, that the rules should give even more deference to state law, questioning in particular the definitions and the proposed addition to the "other purposes" criterion for exception determinations in this regard.

Response: With respect to the exception process provided for by section 1178(a)(2)(A), the contention that the HIPAA standards should uniformly control is an argument that should be addressed to the Congress, not this agency. Section 1178 of the Act expressly gives the Secretary authority to grant exceptions to the general rule that the HIPAA standards preempt contrary state law in the circumstances she determines come within the provisions at section 1178(a)(2)(A). We agree that the underlying statutory goal of standardizing financial and administrative health care transactions dictates that exceptions should be granted only on narrow grounds. Nonetheless, Congress clearly intended to accommodate some state laws in these areas, and the Department is not free to disregard this Congressional choice. As is more fully explained below, we have interpreted the statutory criteria for exceptions under section 1178(a)(2)(A) to balance the need for relative uniformity with respect to the HIPAA standards with state needs to set certain policies in the statutorily defined areas. The situation is different with respect to state laws relating to the privacy of protected health information. Many of the comments arguing for uniform standards were particularly concerned with discrepancies between the federal privacy standards and various state privacy requirements. Unlike the situation with respect to the transactions standards, where states have generally not entered the field, all states regulate the privacy of some medical information to a greater or lesser extent. Thus, we understand the private sector's concern at having to reconcile differing state and federal privacy requirements. This is, however, likewise an area where the policy choice has been made by Congress. Under section 1178(a)(2)(B) of the Act and section 264(c)(2) of HIPAA, provisions of state privacy laws that are contrary to and more stringent than the corresponding federal standard, requirement, or implementation specification are not preempted. The effect of these provisions is to let the law that is most protective of privacy control (the "federal floor" approach referred to by many commenters), and this policy choice is one with which we agree. Thus, the statute makes it impossible for the Secretary to accommodate the requests to establish uniformly controlling federal privacy standards, even if doing so were viewed as desirable.

Comment: Numerous comments stated support for the proposal at proposed Subpart B to issue advisory opinions with respect to the preemption of state laws

1/3/2003

relating to the privacy of individually identifiable health information. A number of these comments appeared to assume that the Secretary's advisory opinions would be dispositive of the issue of whether or not a state law was preempted. Many of these commenters suggested what they saw as improvements to the proposed process, but supported the proposal to have the Department undertake this function. Response: Despite the general support for the advisory opinion proposal, we decided not to provide specifically for the issuance of such opinions. The following considerations led to this decision. First, the assumption by commenters that an advisory opinion would establish what law applied in a given situation and thereby simplify the task of ascertaining what legal requirements apply to a covered entity or entities is incorrect. Any such opinion would be advisory only. Although an advisory opinion issued by the Department would indicate to covered entities how the Department would resolve the legal conflict in question and would apply the law in determining compliance, it would not bind the courts. While we assume that most courts would give such opinions deference, the outcome could not be guaranteed. Second, the thousands of questions raised in the public comment about the interpretation, implications, and consequences of all of the proposed regulatory provisions have led us to conclude that significant advice and technical assistance about all of the regulatory requirements will have to be provided on an ongoing basis. We recognize that the preemption concerns that would have been addressed by the proposed advisory opinions were likely to be substantial. However, there is no reason to assume that they will be the most substantial or urgent of the questions that will most likely need to be addressed. It is our intent to provide as much technical advice and assistance to the regulated community as we can with the resources available. Our concern is that setting up an advisory opinion process for just one of the many types of issues that will have to be addressed will lead to a non-optimal allocation of those resources. Upon careful consideration, therefore, we have decided that we will be better able to prioritize our workload and be better able to be responsive to the most urgent and substantial questions raised to the Department, if we do not provide for a formal advisory opinion process on preemption as proposed. Comment: A few commenters argued that the Privacy Rule should preempt state laws that would impose more stringent privacy requirements for the conduct of clinical trials. One commenter asserted that the existing federal regulations and guidelines for patient informed consent, together with the proposed rule, would adequately protect patient privacy.

Response: The Department does not have the statutory authority under HIPAA to preempt state laws that would impose more stringent privacy requirements on covered entities. HIPAA provides that the rule promulgated by the Secretary may not preempt state laws that are in conflict [82581 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] with the regulatory requirements and that provide greater privacy protections.

Section 160.201—Applicability

1/3/2003

Comment: Several commenters indicated that the guidance provided by the definitions at proposed § 160.202 would be of substantial benefit both to regulated entities and to the public. However, these commenters argued that the applicability of such definitions would be too limited as drafted, since proposed § 160.201 provided that the definitions applied only to “determinations and advisory opinions issued by the Secretary pursuant to 42 U.S.C. 1320d–7.” The commenters stated that it would be far more helpful to make the definitions in proposed § 160.202 more broadly applicable, to provide general guidance on the issue of preemption.

Response: We agree with the comments on this issue, and have revised the applicability provision of subpart B below accordingly. Section 160.201 below sets out that Subpart B implements section 1178. This means, in our view, that the definitions of the statutory terms at § 160.202 are legislative rules that apply when those statutory terms are employed, whether by HHS, covered entities, or the courts.

Section 160.202—Definitions

Contrary

Comment: Some commenters asserted that term “contrary” as defined at § 160.202 was overly broad and that its application would be time-consuming and confusing for states. These commenters argued that, under the proposed definition, a state would be required to examine all of its laws relating to health information privacy in order to determine whether or not its law were contrary to the requirements proposed. It was also suggested that the definition contain examples of how it would work in practical terms. A few commenters, however, argued that the definition of “contrary” as proposed was too narrow. One commenter argued that the Secretary erred in her assessment of the case law analyzing what is known as “conflict preemption” and which is set forth in shorthand in the tests set out at § 160.202.

Response: We believe that the definition proposed represents a policy that is as clear as is feasible and which can be applied nationally and uniformly. As was noted in the preamble to the proposed rules (at 64 FR 59997), the tests in the proposed definition of “contrary” are adopted from the jurisprudence of “conflict preemption.” Since preemption is a judicially developed doctrine, it is reasonable to interpret this term as indicating that the statutory analysis should tie in to the analytical formulations employed by the courts. Also, while the court-developed tests may not be as clear as commenters would like, they represent a long-term, thoughtful consideration of the problem of defining when a state/federal conflict exists. They will also, we assume, generally be employed by the courts when conflict issues arise under the rules below. We thus see no practical alternative to the proposed definition and have retained it unchanged. With respect to various suggestions for shorthand versions of the proposed tests, such as the arguably broader term “inconsistent with,” we see no operational advantages to such terms.

Comment: One comment asked that the Department clarify that if state law is not preempted, then the federal law would not also apply.

1/3/2003

Response: This comment raises two issues, both of which deserve discussion. First, a state law may not be preempted because there is no conflict with the analogous federal requirement; in such a situation, both laws can, and must, be complied with. We thus do not accept this suggestion, to the extent that it suggests that the federal law would give way in this situation. Second, a state law may also not be preempted because it comes within section 1178(a)(2)(B), section 1178(b), or section 1178(c); in this situation, a contrary federal law would give way.

Comment: One comment urged the Department to take the position that where state law exists and no analogous federal requirement exists, the state requirement would not be “contrary to” the federal requirement and would therefore not trigger preemption.

Response: We agree with this comment.

Comment: One commenter criticized the definition as unhelpful in the multistate transaction context. For example, it was asked whether the issue of whether a state law was “contrary to” should be determined by the law of the state where the treatment is provided, where the claim processor is located, where the payment is issued, or the data maintained, assuming all are in different states.

Response: This is a choice of law issue, and, as is discussed more fully below, is a determination that is routinely made today in connection with multi-state transactions. See discussion below under Exception Determinations (Criteria for Exception Determinations).

State Law

Comment: Comments noted that the definition of “state law” does not explicitly include common law and recommended that it be revised to do so or to clarify that the term includes evidentiary privileges recognized at state law. Guidance concerning the impact of state privileges was also requested.

Response: As requested, we clarify that the definition of “state law” includes common law by including the term “common law.” In our view, this phrase encompasses evidentiary privileges recognized at state law (which may also, we note, be embodied in state statutes).

Comment: One comment criticized this definition as unwieldy, in that locating state laws pertaining to privacy is likely to be difficult. It was noted that Florida, for example, has more than 60 statutes that address health privacy.

Response: To the extent that state laws currently apply to covered entities, they have presumably determined what those laws require in order to comply with them. Thus, while determining which laws are “contrary” to the federal requirements will require additional work in terms of comparing state law with the federal requirements, entities should already have acquired the knowledge of state law needed for this task in the ordinary course of doing business.

Comment: The New York City Department of Health noted that in many cases, provisions of New York State law are inapplicable within New York City, because the state legislature has recognized that the local code is tailored to the particular needs

1/3/2003

of the City. It urged that the New York City Code be treated as state law, for preemption purposes.

Response: We agree that, to the extent a state treats local law as substituting for state law it could be considered to be “state law” for purposes of this definition. If, however, a local law is local in scope and effect, and a tier of state law exists over the same subject matter, we do not think that the local law could or should be treated as “state law” for preemption purposes. We do not have sufficient information to assess the situation raised by this comment with respect to this principle, and so express no opinion thereon.

More Stringent

Comment: Many commenters supported the policy in the proposed definition of “individual” at proposed § 164.502, which would have permitted unemancipated minors to exercise, on [82582 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] their own behalf, rights granted to individuals in cases where they consented to the underlying health care.

Commenters stated, however, that the proposed preemption provision would leave in place state laws authorizing or prohibiting disclosure to parents of the protected health information of their minor children and would negate the proposed policy for the treatment of minors under the rule. The comments stated that such state laws should be treated like other state laws, and preempted to the extent that they are less protective of the privacy of minors. Other commenters supported the proposed preemption provision—not to preempt a state law to the extent it authorizes or prohibits disclosure of protected health information regarding a minor to a parent.

Response: Laws regarding access to health care for minors and confidentiality of their medical records vary widely; this regulation recognizes and respects the current diversity of state law in this area. Where states have considered the balance involved in protecting the confidentiality of minors’ health information and have explicitly acted, for example, to authorize disclosure, defer the decision to disclose to the discretion of the health care provider, or prohibit disclosure of minor’s protected health information to a parent, the rule defers to these decisions to the extent that they regulate such disclosures.

Comment: The proposed definition of “more stringent” was criticized as affording too much latitude to for granting exceptions for state laws that are not protective of privacy. It was suggested that the test should be “most protective of the individual’s privacy.”

Response: We considered adopting this test. However, for the reasons set out at 64 FR 59997, we concluded that this test would not provide sufficient guidance. The comments did not address the concerns we raised in this regard in the preamble to the proposed rules, and we continue to believe that they are valid.

Comment: A drug company expressed concern with what it saw as the expansive definition of this term, arguing that state governments may have less experience with the special needs of researchers than federal agencies and may unknowingly adopt

1/3/2003

laws that have a deleterious effect on research. A provider group expressed concern that allowing stronger state laws to prevail could result in diminished ability to get enough patients to complete high quality clinical trials.

Response: These concerns are fundamentally addressed to the “federal floor” approach of the statute, not to the definition proposed: even if the definition of “more stringent” were narrowed, these concerns would still exist. As discussed above, since the “federal floor” approach is statutory, it is not within the Secretary’s authority to change the dynamics that are of concern.

Comment: One comment stated that the proposed rule seemed to indicate that the “more stringent” and “contrary to” definitions implied that these standards would apply to ERISA plans as well as to non-ERISA plans.

Response: The concern underlying this comment is that ERISA plans, which are not now subject to certain state laws because of the “field” preemption provision of ERISA but which are subject to the rules below, will become subject to state privacy laws that are “more stringent” than the federal requirements, due to the operation of section 1178(a)(2)(B), together with section 264(c)(2). We disagree that this is the case. While the courts will have the final say on these questions, it is our view that these sections simply leave in place more stringent state laws that would otherwise apply; to the extent that such state laws do not apply to ERISA plans because they are preempted by ERISA, we do not think that section 264(c)(2) overcomes the preemption effected by section 514(a) of ERISA. For more discussion of this point, see 64 FR 60001.

Comment: The Lieutenant Governor’s Office of the State of Hawaii requested a blanket exemption for Hawaii from the federal rules, on the ground that its recently enacted comprehensive health privacy law is, as a whole, more stringent than the proposed federal standards. It was suggested that, for example, special weight should be given to the severity of Hawaii’s penalties. It was suggested that a new definition (“comprehensive”) be added, and that “more stringent” be defined in that context as whether the state act or code as a whole provides greater protection. An advocacy group in Vermont argued that the Vermont legislature was poised to enact stronger and more comprehensive privacy laws and stated that the group would resent a federal prohibition on that.

Response: The premise of these comments appears to be that the provision-by-provision approach of Subpart B, which is expressed in the definition of the term “contrary”, is wrong. As we explained in the preamble to the proposed rules (at 64 FR 59995), however, the statute dictates a provision-by-provision comparison of state and federal requirements, not the overall comparison suggested by these comments. We also note that the approach suggested would be practically and analytically problematic, in that it would be extremely difficult, if not impossible, to determine what is a legitimate stopping point for the provisions to be weighed on either the state side or the federal side of the scale in determining which set of laws was the “more stringent.” We accordingly do not accept the approach suggested by these comments. With respect to the comment of the Vermont group, nothing in the rules below prohibits or places any limits on states enacting stronger or more

1/3/2003

comprehensive privacy laws. To the extent that states enact privacy laws that are stronger or more comprehensive than contrary federal requirements, they will presumably not be preempted under section 1178(a)(2)(B). To the extent that such state laws are not contrary to the federal requirements, they will act as an overlay on the federal requirements and will have effect.

Comment: One comment raised the issue of whether a private right of action is a greater penalty, since the proposed federal rule has no comparable remedy.

Response: We have reconsidered the proposed “penalty” provision of the proposed definition of “more stringent” and have eliminated it. The HIPAA statute provides for only two types of penalties: fines and imprisonment. Both types of penalties could be imposed in addition to the same type of penalty imposed by a state law, and should not interfere with the imposition of other types of penalties that may be available under state law. Thus, we think it is unlikely that there would be a conflict between state and federal law in this respect, so that the proposed criterion is unnecessary and confusing. In addition, the fact that a state law allows an individual to file a lawsuit to protect privacy does not conflict with the HIPAA penalty provisions.

*Relates to the Privacy of Individually
Identifiable Health Information*

Comment: One comment criticized the definition of this term as too narrow in scope and too uncertain. The commenter argued that determining the specific purpose of a state law may be difficult and speculative, because many state laws have incomplete, inaccessible, or non-existent legislative histories. It was suggested that the definition be revised by deleting the word “specific” before the word “purpose.” Another commenter argued [82583 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] that the definition of this term should be narrowed to minimize reverse preemption by more stringent state laws. One commenter generally supported the proposed definition of this term.

Response: We are not accepting the first comment. The purpose of a given state enactment should be ascertainable, if not from legislative history or a purpose statement, then from the statute viewed as a whole. The same should be true of state regulations or rulings. In any event, it seems appropriate to restrict the field of state laws that may potentially trump the federal standards to those that are clearly intended to establish state public policy and operate in the same area as the federal standards. To the extent that the definition in the rules below does this, we have accommodated the second comment. We note, however, that we do not agree that the definition should be further restricted to minimize “reverse preemption,” as suggested by this comment, as we believe that state laws that are more protective of privacy than contrary federal standards should remain, in order to ensure that the privacy of individuals’ health information receives the maximum legal protection available.

Sections 160.203 and 160.204—

1/3/2003

Exception Determinations and Advisory Opinions

Most of the comments received on proposed Subpart B lumped together the proposed process for exception determinations under section 1178(a)(2)(A) with the proposed process for issuing advisory opinions under section 1178(a)(2)(B), either because the substance of the comment applied to both processes or because the commenters did not draw a distinction between the two processes. We address these general comments in this section.

Comment: Numerous commenters, particularly providers and provider groups, recommended that exception determinations and advisory opinions not be limited to states and advocated allowing all covered entities (including individuals, providers and insurers), or private sector organizations, to request determinations and opinions with respect to preemption of state laws. Several commenters argued that limiting requests to states would deny third party stakeholders, such as life and disability income insurers, any means of resolving complex questions as to what rule they are subject to. One commenter noted that because it is an insurer who will be liable if it incorrectly analyzes the interplay between laws and reaches an incorrect conclusion, there would be little incentive for the states to request clarification. It would also cause large administrative burdens which, it was stated, would be costly and confusing. It was also suggested that the request for the exception be made to the applicable state's attorney general or chief legal officer, as well as the Secretary. Various changes to the language were suggested, such as adding that "a covered entity, or any other entity impacted by this rule" be allowed to submit the written request.

Response: We agree, and have changed § 164.204(a) below accordingly. The decision to eliminate advisory opinions makes this issue moot with respect to those opinions.

Comment: Several commenters noted that it was unclear under the proposed rule which state officials would be authorized to request a determination.

Response: We agree that the proposed rule was unclear in this respect. The final rule clarifies who may make the request for a state, with respect to exception determinations. See, § 160.204(a). The language adopted should ensure that the Secretary receives an authoritative statement from the state. At the same time, this language provides states with flexibility, in that the governor or other chief elected official may choose to designate other state officials to make such requests.

Comment: Many commenters recommended that a process be established whereby HHS performs an initial state-by-state critical analysis to provide guidance on which state laws will not be preempted; most suggested that such an analysis (alternatively referred to as a database or clearinghouse) should be completed before providers would be required to come into compliance. Many of these comments argued that the Secretary should bear the cost for the analyses of state law, disagreeing with the premise stated in the preamble to the proposed rules that it is more efficient for the private market to complete the state-by-state review. Several comments also

1/3/2003

requested that HHS continue to maintain and monitor the exception determination process, and update the database over time in order to provide guidance and certainty on the interaction of the federal rules with newly enacted or amended state laws that are produced after the final rule. Some comments recommended that each state be required to certify agreement with the HHS analyses. In contrast, one hospital association noted concerns that the Secretary would conduct a nationwide analysis of state laws. The comment stated that implementation would be difficult since much of the law is a product of common law, and such state-specific research should only be attempted by experienced health care attorneys in each jurisdiction. Response: These comments seem to be principally concerned with potential conflicts between state privacy laws and the privacy standards, because, as is more fully explained below, preemption of contrary state laws not relating to privacy is automatic unless the Secretary affirmatively acts under section 1178(a)(2)(A) to grant an exception. We recognize that the provisions of sections 1178(b) (state public health laws), and 1178(c) (state regulation of health plans) similarly preserve state laws in those areas, but very little of the public comment appeared to be concerned with these latter statutory provisions. Accordingly, we respond below to what we see as the commenters' main concern. The Department will not do the kind of global analysis requested by many of these comments. What these comments are in effect seeking is a global advisory opinion as to when the federal privacy standards will control and when they will not. We understand the desire for certainty underlying these comments. Nonetheless, the reasons set out above as the basis for our decision not to establish a formal advisory opinion process apply equally to these requests. We also do not agree that the task of evaluating the requirements below in light of existing state law is unduly burdensome or unreasonable. Rather, it is common for new federal requirements to necessitate an examination by the regulated entities of the interaction between existing state law and the federal requirements incident to coming into compliance. We agree, however, that the case is different where the Secretary has affirmatively acted, either through granting an exception under section 1178(a)(2)(A) or by making a specific determination about the effect of a particular state privacy law in, for example, the course of determining an entity's compliance with the privacy standards. As is discussed below, the Department intends to make notice of exception determinations that it makes routinely available. We do not agree with the comments suggesting that compliance by covered entities be delayed pending completion of an analysis by the Secretary and that states be required to certify agreement with the Secretary's analysis, as we are not institutionalizing the advisory opinion/analysis process upon which these comments are predicated. [82584 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] Furthermore, with respect to the suggestion regarding delaying the compliance date, Congress provided in section 1175(b) of the Act for a delay in when compliance is required to accommodate the needs of covered entities to address implementation issues such as those raised by these comments. With respect to the suggestion regarding requiring states to certify their agreement with the Secretary's analysis, we have no authority to do this.

1/3/2003

Comment: Several commenters criticized the proposed provision for annual publication of determinations and advisory opinions in the Federal Register as inadequate. They suggested that more frequent notices should be made and the regulation be changed accordingly, to provide for publication either quarterly or within a few days of a determination. A few commenters suggested that any determinations made, or opinions issued, by the Secretary be published on the Department's website within 10 days or a few days of the determination or opinion.

Response: We agree that the proposed provision for annual publication was inadequate and have accordingly deleted it. Subpart B contains no express requirement for publication, as the Department is free to publish its determinations absent such a requirement. It is our intention to publish notice of exception determinations on a periodic basis in the Federal Register. We will also consider other avenues of making such decisions publicly available as we move into the implementation process.

Comment: A few commenters argued that the process for obtaining an exception determination or an advisory opinion from the Secretary will result in a period of time in which there is confusion as to whether state or federal law applies. The proposed regulations say that the federal provisions will remain effective until the Secretary makes a determination concerning the preemption issue. This means that, for example, a state law that was enacted and enforced for many years will be preempted by federal law for the period of time during which it takes the Secretary to make a determination. Then if the Secretary determines that the state law is not preempted, the state law will again become effective. Such situations will result in confusion and unintended violations of the law. One of the commenters suggested that requests for exceptions be required only when a challenge is brought against a particular state law, and that a presumption of validity should lie with state laws. Another commenter, however, urged that "instead of the presumption of preemption, the state laws in question would be presumed to be subject to the exception unless or until the Secretary makes a determination to the contrary."

Response: It is true that the effect of section 1178(a)(2)(A) is that the federal standards will preempt contrary state law and that such preemption will not be removed unless and until the Secretary acts to grant an exception under that section (assuming, of course, that another provision of section 1178 does not apply). We do not agree, however, that confusion should result, where the issue is whether a given state law has been preempted under section 1178(a)(2)(A). Because preemption is automatic with respect to state laws that do not come within the other provisions of section 1178 (i.e., sections 1178(a)(2)(B), 1178(b), and 1178(c)), such state laws are preempted until the Secretary affirmatively acts to preserve them from preemption by granting an exception under section 1178(a)(2)(A). We cannot accept the suggestion that a presumption of validity attach to state laws, and that states not be required to request exceptions except in very narrow circumstances. The statutory scheme is the opposite: The statute effects preemption in the section 1178(a)(2)(A) context unless the Secretary affirmatively acts to except the contrary state law in question. With respect to preemption under sections 1178(b) and 1178(c) (the carveouts for

1/3/2003

state public health laws and state regulation of health plans), we do not agree that preemption is likely to be a major cause of uncertainty. We have deferred to Congressional intent by crafting the permissible releases for public health, abuse, and oversight broadly. See, §§ 164.512(b)—(d) below. Since there must first be a conflict between a state law and a federal requirement in order for an issue of preemption to even arise, we think that, as a practical matter, few preemption questions should arise with respect to sections 1178(b) and 1178(c). With respect to preemption of state privacy laws under section 1178(a)(2)(B), however, we agree that the situation may be more difficult to ascertain, because the Secretary does not determine the preemption status of a state law under that section, unlike the situation with respect to section 1178(a)(2)(A). We have tried to define the term “more stringent” to identify and particularize the factors to be considered by courts to those relevant to privacy interests. The more specific (than the statute) definition of this term at § 160.202 below should provide some guidance in making the determination as to which law prevails. Ambiguity in the state of the law might also be a factor to be taken into account in determining whether a penalty should be applied.

Comment: Several comments recommended that exception determinations or advisory opinions encompass a state act or code in its entirety (in lieu of a provision-specific evaluation) if it is considered more stringent as a whole than the regulation. It was argued that since the provisions of a given law are typically interconnected and related, adopting or overriding them on a provision-by-provision basis would result in distortions and/or unintended consequences or loopholes. For example, when a state law includes authorization provisions, some of which are consistent with the federal requirements and some which are not, the cleanest approach is to view the state law as inconsistent with the federal requirements and thus preempted in its entirety. Similarly, another comment suggested that state confidentiality laws written to address the specific needs of individuals served within a discreet system of care be considered as a whole in assessing whether they are as stringent or more stringent than the federal requirements. Another comment requested explicit clarification that state laws with a broader scope than the regulation will be viewed as more stringent and be allowed to stand.

Response: We have not adopted the approach suggested by these comments. As discussed above with respect to the definition of the term “more stringent,” it is our view that the statute precludes the approach suggested. We also suggest that this approach ignores the fact that each separate provision of law usually represents a nuanced policy choice to, for example, permit this use or prohibit that disclosure; the aggregated approach proposed would fail to recognize and weigh such policy choices.

Comment: One comment recommended that the final rule: permit requests for exception determinations and advisory opinions as of the date of publication of the final rule, require the Secretary to notify the requestor within a specified short period of time of all additional information needed, and prohibit enforcement action until the Secretary issues a response.

1/3/2003

Response: With respect to the first recommendation, we clarify that requests for exception determinations may be made at any time; since the process for issuing advisory opinions has not been adopted, this recommendation is moot as it pertains [82585 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] to advisory opinions. With respect to the second recommendation, we will undertake to process exception requests as expeditiously as possible, but, for the reasons discussed below in connection with the comments relating to setting deadlines for those determinations, we cannot commit at this time to a “specified short period of time” within which the Secretary may request additional information. We see no reason to agree to the third recommendation. Because contrary state laws for which an exception is available only under section 1178(a)(2)(A) will be preempted by operation of law unless and until the Secretary acts to grant an exception, there will be an ascertainable compliance standard for compliance purposes, and enforcement action would be appropriate where such compliance did not occur.

*Sections 160.203(a) and 160.204(a)—
Exception Determinations*

*Section 160.203(a)—Criteria for
Exception Determinations*

Comment: Numerous comments criticized the proposed criteria for their substance or lack thereof. A number of commenters argued that the effectiveness language that was added to the third statutory criterion made the exception so massive that it would swallow the rule. These comments generally expressed concern that laws that were less protective of privacy would be granted exceptions under this language. Other commenters criticized the criteria generally as creating a large loophole that would let state laws that do not protect privacy trump the federal privacy standards.

Response: We agree with these comments. The scope of the statutory criteria is ambiguous, but they could be read so broadly as to largely swallow the federal protections. We do not think that this was Congress’s intent. Accordingly, we have added language to most of the statutory criteria clarifying their scope. With respect to the criteria at 1178(a)(2)(A)(i), this clarifying language generally ties the criteria more specifically to the concern with protecting and making more efficient the health care delivery and payment system that underlies the Administrative Simplification provisions of HIPAA, but, with respect to the catch-all provision at section 1178(a)(2)(A)(i)(IV), also requires that privacy interests be balanced with such concerns, to the extent relevant. We require that exceptions for rules to ensure appropriate state regulation of insurance and health plans be stated in a statute or regulation, so that such exceptions will be clearly tied to statements of priorities made by publicly accountable bodies (e.g., through the public comment process for regulations, and by elected officials through statutes). With respect to the criterion at section 1178(a)(2)(A)(ii), we have further delineated what “addresses controlled

1/3/2003

substances” means. The language provided, which builds on concepts at 21 U.S.C. 821 and the Medicare regulations at 42 CFR 1001.2, delineates the area within which the government traditionally regulates controlled substances, both civilly and criminally; it is our view that HIPAA was not intended to displace such regulation.

Comment: Several commenters urged that the request for determination by the Secretary under proposed § 160.204(a) be limited to cases where an exception is absolutely necessary, and that in making such a determination, the Secretary should be required to make a determination that the benefits of granting an exception outweigh the potential harm and risk of disclosure in violation of the regulation.

Response: We have not further defined the statutory term “necessary”, as requested. We believe that the determination of what is “necessary” will be fact-specific and context dependent, and should not be further circumscribed absent such specifics. The state will need to make its case that the state law in question is sufficiently “necessary” to accomplish the particular statutory ground for exception that it should trump the contrary federal standard, requirement, or implementation specification.

Comment: One commenter noted that a state should be required to explain whether it has taken any action to correct any less stringent state law for which an exception has been requested. This commenter recommended that a section be added to proposed § 160.204(a) stating that “a state must specify what, if any, action has been taken to amend the state law to comply with the federal regulations.” Another comment, received in the Transactions rulemaking, took the position that exception determinations should be granted only if the state standards in question exceeded the national standards.

Response: The first and last comments appear to confuse the “more stringent” criterion that applies under section 1178(a)(2)(B) of the Act with the criteria that apply to exceptions under section 1178(a)(2)(A). We are also not adopting the language suggested by the first comment, because we do not agree that states should necessarily have to try to amend their state laws as a precondition to requesting exceptions under section 1178(a)(2)(A). Rather, the question should be whether the state has made a convincing case that the state law in question is sufficiently necessary for one of the statutory purposes that it should trump the contrary federal policy.

Comment: One commenter stated that exceptions for state laws that are contrary to the federal standards should not be preempted where the state and federal standards are found to be equal.

Response: This suggestion has not been adopted, as it is not consistent with the statute. With respect to the administrative simplification standards in general, it is clear that the intent of Congress was to preempt contrary state laws except in the limited areas specified as exceptions or carve-outs. See, section 1178. This statutory approach is consistent with the underlying goal of simplifying health care transactions through the adoption of uniform national standards. Even with respect to state laws relating to the privacy of medical information, the statute shields such

1/3/2003

state laws from preemption by the federal standards only if they are “more” stringent than the related federal standard or implementation specification.

Comment: One commenter noted that determinations would apply only to transactions that are wholly intrastate. Thus, any element of a health care transaction that would implicate more than one state’s law would automatically preclude the Secretary’s evaluation as to whether the laws were more or less stringent than the federal requirement. Other commenters expressed confusion about this proposed requirement, noting that providers and plans operate now in a multi-state environment.

Response: We agree with the commenters and have dropped the proposed requirement. As noted by the commenters, health care entities now typically operate in a multi-state environment, so already make the choice of law judgements that are necessary in multi-state transactions. It is the result of that calculus that will have to be weighed against the federal standards, requirements, and implementation specifications in the preemption analysis.

Comment: One comment received in the Transactions rulemaking suggested that the Department should allow exceptions to the standard transactions to accommodate abbreviated transactions between state agencies, such as claims between a public health department and the state Medicaid [82586 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] agency. Another comment requested an exception for Home and Community Based Waiver Services from the transactions standards.

Response: The concerns raised by these comments would seem to be more properly addressed through the process established for maintaining and modifying the transactions standards. If the concerns underlying these comments cannot be addressed in this manner, however, there is nothing in the rules below to preclude states from requesting exceptions in such cases. They will then have to make the case that one or more grounds for exception applies.

Section 160.204(a)—Process for Exception Determinations—Comments and Responses

Comment: Several comments received in the Transactions rulemaking stated that the process for applying for and granting exception determinations (referred to as “waivers” by some) needed to be spelled out in the final rule.

Response: We agree with these comments. As noted above, since no process was proposed in the Transactions rulemaking, a process for making exception determinations was not adopted in those final rules. Subpart B below adopts a process for making exception determinations, which responds to these comments.

Comment: Comments stated that the exception process would be burdensome, unwieldy, and time consuming for state agencies as well as the Department. One comment took the position that states should not be required to submit exception requests to the Department under proposed § 160.203(a), but could provide

1/3/2003

documentation that the state law meets one of the conditions articulated in proposed § 160.203.

Response: We disagree that the process adopted at § 164.204 below will be burdensome, unwieldy, or time consuming. The only thing the regulation describes is the showings that a requestor must make as part of its submission, and all are relevant to the issue to be determined by the Secretary. How much information is submitted is, generally speaking, in the requestor's control, and the regulation places no restrictions on how the requestor obtains it, whether by acting directly, by working with providers and/or plans, or by working with others. With respect to the suggestion that states not be required to submit exception requests, we disagree that this suggestion is either statutorily authorized or advisable. We read this comment as implicitly suggesting that the Secretary must proactively identify instances of conflict and evaluate them. This suggestion is, thus, at bottom the same as the many suggestions that we create a database or compendium of controlling law, and it is rejected for the same reasons.

Comment: Several comments urged that all state requests for nonpreemption include a process for public participation. These comments believe that members of the public and other interested stakeholders should be allowed to submit comments on a state's request for exception, and that these comments should be reviewed and considered by the Secretary in determining whether the exception should be granted. One comment suggested that the Secretary at least give notice to the citizens of the state prior to granting an exception.

Response: The revision to § 160.204(a), to permit requests for exception determinations by any person, responds to these comments.

Comment: Many commenters noted that the lack of a clear and reasonable time line for the Secretary to issue an exception determination would not provide sufficient assurance that the questions regarding what rules apply will be resolved in a time frame that will allow business to be conducted properly, and argued that this would increase confusion and uncertainty about which statutes and regulations should be followed. Timeframes of 60 or 90 days were suggested. One group suggested that, if a state does not receive a response from HHS within 60 days, the waiver should be deemed approved.

Response: The workload prioritization and management considerations discussed above with respect to advisory opinions are also relevant here and make us reluctant to agree to a deadline for making exception determinations. This is particularly true at the outset, since we have no experience with such requests. We therefore have no basis for determining how long processing such requests will take, how many requests we will need to process, or what resources will be available for such processing. We agree that states and other requesters should receive timely responses and will make every effort to make determinations as expeditiously as possible, but we cannot commit to firm deadlines in this initial rule. Once we have experience in handling exception requests, we will consult with states and others in regard to their experiences and concerns and their suggestions for improving the Secretary's expeditious handling of such requests. We are not accepting the

1/3/2003

suggestion that requests for exception be deemed approved if not acted upon in some defined time period. Section 1178(a)(2)(A) requires a specific determination by the Secretary. The suggested policy would not be consistent with this statutory requirement. It is also inadvisable from a policy standpoint, in that it would tend to maximize exceptions. This would be contrary to the underlying statutory policy in favor of uniform federal standards.

Comment: One commenter took exception to the requirement for states to seek a determination from the Department that a provision of state law is necessary to prevent fraud and abuse or to ensure appropriate state regulation of insurance plans, contending that this mandate could interfere with the Insurance Commissioners' ability to do their jobs. Another commenter suggested that the regulation specifically recognize the broad scope of state insurance department activities, such as market conduct examinations, enforcement investigations, and consumer complaint handling.

Response: The first comment raises an issue that lies outside our legal authority to address, as section 1178(a)(2)(A) clearly mandates that the Secretary make a determination in these areas. With respect to the second comment, to the extent these concerns pertain to health plans, we believe that the provisions at § 164.512 relating to oversight and disclosures required by law should address the concerns underlying this comment.

Section 160.204(a)(4)—Period of Effectiveness of Exception Determinations

Comment: Numerous commenters stated that the proposed three year limitation on the effectiveness of exception determinations would pose significant problems and should be limited to one year, since a one year limitation would provide more frequent review of the necessity for exceptions. The commenters expressed concern that state laws which provide less privacy protection than the federal regulation would be given exceptions by the Secretary and thus argued that the exceptions should be more limited in duration or that the Secretary should require that each request, regardless of duration, include a description of the length of time such an exception would be needed. One state government commenter, however, argued that the 3 year limit should be eliminated entirely, on the ground that requiring a redetermination [82587 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] every three years would be burdensome for the states and be a waste of time and resources for all parties. Other commenters, including two state agencies, suggested that the exemption should remain effective until either the state law or the federal regulation is changed. Another commenter suggested that the three year sunset be deleted and that the final rule provide for automatic review to determine if changes in circumstance or law would necessitate amendment or deletion of the opinion. Other recommendations included deeming the state law as continuing in effect upon the submission of a state application for an

1/3/2003

exemption rather than waiting for a determination by the Secretary that may not occur for a substantial period of time.

Response: We are persuaded that the proposed 3 year limit on exception determinations does not make sense where neither law providing the basis for the exception has changed in the interim. We also agree that where either law has changed, a previously granted exception should not continue. Section 160.205(a) below addresses these concerns.

*Sections 160.203(b) and 160.204(b)—
Advisory Opinions*

*Section 160.203(b)—Effect of Advisory
Opinions*

Comment: Several commenters questioned whether or not DHHS has standing to issue binding advisory opinions and recommended that the Department clarify this issue before implementation of this regulation. One respondent suggested that the Department clarify in the final rule the legal issues on which it will opine in advisory opinion requests, and state that in responding to requests for advisory opinions the Department will not opine on the preemptive force of ERISA with respect to state laws governing the privacy of individually identifiable health information, since interpretations as to the scope and extent of ERISA's preemption provisions are outside of the Department's jurisdictional authority. One commenter asked whether a state could enforce a state law which the Secretary had indicated through an advisory opinion is preempted by federal law. This commenter also asked whether the state would be subject to penalties if it chose to continue to enforce its own laws.

Response: As discussed above, in part for reasons raised by these comments, the Department has decided not to have a formal process for issuing advisory opinions, as proposed. Several of these concerns, however, raise issues of broader concern that need to be addressed. First, we disagree that the Secretary lacks legal authority to opine on whether or not state privacy laws are preempted. The Secretary is charged by law with determining compliance, and where state law and the federal requirements conflict, a determination of which law controls will have to be made in order to determine whether the federal standard, requirement, or implementation specification at issue has been violated. Thus, the Secretary cannot carry out her enforcement functions without making such determinations. It is further reasonable that, if the Secretary makes such determinations, she can make those determinations known, for whatever persuasive effect they may have. The questions as to whether a state could enforce, or would be subject to penalties if it chose to continue to enforce, its own laws following a denial by the Secretary of an exception request under § 160.203 or a holding by a court of competent jurisdiction that a state privacy law had been preempted by a contrary federal privacy standard raise several issues. **First, a state law is preempted under the Act only to the extent that it applies to covered entities; thus, a state is free to continue to enforce a "preempted" state**

1/3/2003

law against non-covered entities to which the state law applies. If there is a question of coverage, states may wish to establish processes to ascertain which entities within their borders are covered entities within the meaning of these rules. Second, with respect to covered entities, if a state were to try to enforce a preempted state law against such entities, it would presumably be acting without legal authority in so doing. We cannot speak to what remedies might be available to covered entities to protect themselves against such wrongful state action, but we assume that covered entities could seek judicial relief, if all else failed. With respect to the issue of imposing penalties on states, we do not see this as likely. The only situation that we can envision in which penalties might be imposed on a state would be if a state agency were itself a covered entity and followed a preempted state law, thereby violating the contrary federal standard, requirement, or implementation specification.

*Section 160.204(b)—Process for
Advisory Opinions*

Comment: Several commenters stated that it was unclear whether a state would be required to submit a request for an advisory opinion in order for the law to be considered more stringent and thus not preempted. The Department should clarify whether a state law could be non-preempted even without such an advisory opinion. Another commenter requested that the final rule explicitly state that the stricter rule always applies, whether it be state or federal, and regardless of whether there is any conflict between state and federal law.

Response: The elimination of the proposed process for advisory opinions renders moot the first question. Also, the preceding response clarifies that which law preempts in the privacy context (assuming that the state law and federal requirement are “contrary”) is a matter of which one is the “more stringent.” This is not a matter which the Secretary will ultimately determine; rather, this is a question about which the courts will ultimately make the final determination. With respect to the second comment, we believe that § 160.203(b) below responds to this issue, but we would note that the statute already provides for this.

Comment: Several commenters supported the decision to limit the parties who may request advisory opinions to the state. These commenters did not believe that insurers should be allowed to request an advisory opinion and open every state law up to challenge and review. Several commenters requested that guidance on advisory opinions be provided in all circumstances, not only at the Secretary’s discretion. It was suggested that proposed § 160.204(b)(2)(iv) be revised to read as follows: “A state may submit a written request to the Secretary for an advisory opinion under this paragraph. The request must include the following information: the reasons why the state law should or should not be preempted by the federal standard, requirement, or implementation specification, including how the state law meets the criteria at § 160.203(b).”

Response: The decision not to have a formal process for issuing advisory opinions renders these issues moot.

1/3/2003

*Sections 160.203(c) and 160.203(d)—
Statutory Carve-Outs*

Comment: Several commenters asked that the Department provide more specific examples itemizing activities traditionally regulated by the state that could constitute “carve-out” exceptions. These commenters also requested that the Department include language in the regulation stating that if a state law falls within several different exceptions, the state chooses which determination exception shall apply. [82588 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

Response: We are concerned that itemizing examples in this way could leave out important state laws or create inadvertent negative implications that laws not listed are not included. However, as explained above, we have designed the types of activities that are permissive disclosures for public health under § 164.512(b) below in part to come within the carve-out effected by section 1178(b); while the state regulatory activities covered by section 1178(c) will generally come within § 164.512(d) below. With respect to the comments asking that a state get to “choose” which exception it comes under, we have in effect provided for this with respect to exceptions under section 1178(a)(2)(A), by giving the state the right to request an exception under that section. With respect to exceptions under section 1178(a)(2)(B), those exceptions occur by operation of law, and it is not within the Secretary’s power to “let” the state choose whether an exception occurs under that section.

Comment: Several commenters took the position that the Secretary should not limit the procedural requirements in proposed § 160.204(a) to only those applications under proposed § 160.203(a). They urged that the requirements of proposed § 160.204(a) should also apply to preemption under sections 1178(a)(2)(B), 1178(b) and 1178(c). It was suggested that the rules should provide for exception determinations with respect to the matters covered by these provisions of the statute; such additional provisions would provide clear procedures for states to follow and ensure that requests for exceptions are adequately documented. A slightly different approach was taken by several commenters, who recommended that proposed § 160.204(b) be amended to clarify that the Secretary will also issue advisory opinions as to whether a state law constitutes an exception under proposed §§ 160.203(c) and 160.203(d). This change would, they argued, give states the same opportunity for guidance that they have under § 160.203(a) and (b), and as such, avoid costly lawsuits to preserve state laws.

Response: We are not taking either of the recommended courses of action. With respect to the recommendation that we expand the exception determination process to encompass exceptions under sections 1178(a)(2)(B), 1178(b), and 1178(c), we do not have the authority to grant exceptions under these sections. Under section 1178, the Secretary has authority to make exception determinations only with respect to the matters covered by section 1178(a)(2)(A); contrary state laws coming within

1/3/2003

section 1178(a)(2)(B) are preempted if not more stringent, while if a contrary state law comes within section 1178(b) or section 1178(c), it is not preempted. These latter statutory provisions operate by their own terms. Thus, it is not within the Secretary's authority to establish the determination process which these comments seek. With respect to the request seeking advisory opinions in the section 1178(b) and 1178(c) situations, we agree that we have the authority to issue such opinions. However, the considerations described above that have led us not to adopt a formal process for issuing advisory opinions in the privacy context apply with equal force and effect here.

Comment: One commenter argued that it would be unnecessarily burdensome for state health data agencies (whose focus is on the cost of healthcare or improving Medicare, Medicaid, or the healthcare system) to obtain a specific determination from the Department for an exception under proposed § 160.203(c). States should be required only to notify the Secretary of their own determination that such collection is necessary. It was also argued that cases where the statutory carve-outs apply should not require a Secretarial determination.

Response: We clarify that no Secretarial determination is required for activities that fall into one of the statutory carve-outs. With respect to data collections for state health data agencies, we note that provision has been made for many of these activities in several provisions of the rules below, such as the provisions relating to disclosures required by law (§ 164.512(a)), disclosures for oversight (§ 164.512(d)), and disclosures for public health (§ 164.512(b)). Some disclosures for Medicare and Medicaid purposes may also come within the definition of health care operations. A fuller discussion of this issue appears in connection with § 164.512 below.

Constitutional Comments and Responses

Comment: Several commenters suggested that as a general matter the rule is unconstitutional.

Response: We disagree that the rule is unconstitutional. The particular grounds for this conclusion are set out with respect to particular constitutional issues in the responses below. With respect to the comments that simply made this general assertion, the lack of detail of the comments makes a substantive response impossible.

Article II

Comment: One commenter contended that the Secretary improperly delegated authority to private entities by requiring covered entities to enter into contracts with, monitor, and take action for violations of the contract against their business partners. These comments assert that the selection of these entities to "enforce" the regulations violates the Executive Powers Clause and the Appointments and Take Care Clauses.

1/3/2003

Response: We reject the assertion that the business associate provisions constitute an improper delegation of executive power to private entities. HIPAA provides HHS with authority to enforce the regulation against covered entities. The rules below regulate only the conduct of the covered entity; to the extent a covered entity chooses to conduct its funding through a business associate, those functions are still functions of the covered entity. Thus, no improper delegation has occurred because what is being regulated are the actions of the covered entity, not the actions of the business associate in its independent capacity. We also reject the suggestion that the business associates provisions constitute an improper appointment of covered entities to enforce the regulation and violate the Take Care Clause. Because the Secretary has not delegated authority to covered entities, the inference that she has appointed covered entities to exercise such authority misses the mark.

Commerce Clause

Comment: A few commenters suggested that the privacy regulation regulates activities that are not in interstate commerce and which are, therefore, beyond the powers the U.S. Constitution gives the federal government.

Response: We disagree. Health care providers, health plans, and health care clearinghouses are engaged in economic and commercial activities, including the exchange of individually identifiable health information electronically across state lines. These activities constitute interstate commerce. Therefore, they come within the scope of Congress' power to regulate interstate commerce.

Nondelegation Doctrine

Comment: Some commenters objected to the manner by which Congress provided the Secretary authority to promulgate this regulation. These comments asserted that Congress violated the nondelegation doctrine by (1) not providing an "intelligible principle" to guide the agency, (2) not [82589 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] establishing "ascertainable standards," and (3) improperly permitting the Secretary to make social policy decisions.

Response: We disagree. HIPAA clearly delineates Congress' general policy to establish strict privacy protections for individually identifiable health information to encourage electronic transactions. Congress also established boundaries limiting the Secretary's authority. Congress established these limitations in several ways, including by calling for privacy standards for "individually identifiable health information"; specifying that privacy standards must address individuals' rights regarding their individually identifiable health information, the procedures for exercising those rights, and the particular uses and disclosures to be authorized or required; restricting the direct application of the privacy standards to "covered entities," which Congress defined; requiring consultation with the National Committee on Vital and Health Statistics and the Attorney General; specifying the

1/3/2003

circumstances under which the federal requirements would supersede state laws; and specifying the civil and criminal penalties the Secretary could impose for violations of the regulation. These limitations also serve as “ascertainable standards” upon which reviewing courts can rely to determine the validity of the exercise of authority. Although Congress could have chosen to impose expressly an exhaustive list of specifications that must be met in order to achieve the protective purposes of the HIPAA, it was entirely permissible for Congress to entrust to the Secretary the task of providing these specifications based on her experience and expertise in dealing with these complex and technical matters. We disagree with the comments that Congress improperly delegated Congressional policy choices to her. Congress clearly decided to create federal standards protecting the privacy of “individually identifiable health information” and not to preempt state laws that are more stringent. Congress also determined over whom the Secretary would have authority, the type of information protected, and the minimum level of regulation.

Separation of Powers

Comment: Some commenters asserted that the federal government may not preempt state laws that are not as strict as the privacy regulation because to do so would violate the separation of powers in the U.S. Constitution. One comment suggested that the rules raised a substantial constitutional issue because, as proposed, they permitted the Secretary to make determinations on preemption, which is a role reserved for the judiciary.

Response: We disagree. We note that this comment only pertains to determinations under section 1178(a)(2)(A); as discussed above, the rules below provide for no Secretarial determinations with respect to state privacy laws coming within section 1178(a)(2)(B). With respect to determinations under section 1178(a)(2)(A), however, the final rules, like the proposed rules, provide that at a state’s request the Secretary may make certain determinations regarding the preemptive effect of the rules on a particular state law. As usually the case with any administrative decisions, these are subject to judicial review pursuant to the Administrative Procedure Act.

First Amendment

Comment: Some comments suggested that the rules violated the First Amendment. They asserted that if the rule included Christian Science practitioners as covered entities it would violate the separation of church and state doctrine.

Response: We disagree. The First Amendment does not always prohibit the federal government from regulating secular activities of religious organizations. However, we address concerns relating to Christian Science practitioners more fully in the response to comments discussion of the definition of “covered entity” in § 160.103.

Fourth Amendment

1/3/2003

Comment: Many comments expressed Fourth Amendment concerns about various proposed provisions. These comments fall into two categories—general concerns about warrantless searches and specific concerns about administrative searches. Several comments argued that the proposed regulations permit law enforcement and government officials access to protected health information without first requiring a judicial search warrant or an individual’s consent. These comments rejected the applicability of any of the existing exceptions permitting warrantless searches in this context. Another comment argued that federal and state police should be able to obtain personal medical records only with the informed consent of an individual. Many of these comments also expressed concern that protected health information could be provided to government or private agencies for inclusion in a governmental health data system.

Response: We disagree that the provisions of these rules that permit disclosures for law enforcement purposes and governmental health data systems generally violate the Fourth Amendment. The privacy regulation does not create new access rights for law enforcement. Rather, it refrains from placing a significant barrier in front of access rights that law enforcement currently has under existing legal authority. While the regulation may permit a covered entity to make disclosures in specified instances, it does not require the covered entity make the disclosure. Thus, because we are not modifying existing law regarding disclosures to law enforcement officials, except to strengthen the requirements related to requests already authorized under law, and are not requiring any such disclosures, the privacy regulation does not infringe upon individual’s Fourth Amendment rights. We discuss the rationale underlying the permissible disclosures to law enforcement officials more fully in the preamble discussion relating to § 164.512(f). We note that the proposed provision relating to disclosures to government health data systems has been eliminated in the final rule. However, to the extent that the comments can be seen as raising concern over disclosure of protected health information to government agencies for public health, health oversight, or other purposes permitted by the final rule, the reasoning in the previous paragraph applies.

Comment: One commenter suggested that the rules violate the Fourth Amendment by requiring covered entities to provide access to the Secretary to their books, records, accounts, and facilities to ensure compliance with these rules. The commenter also suggested that the requirement that covered entities enter into agreements with their business partners to make their records available to the Secretary for inspection as well also violates the warrant requirement of the Fourth Amendment.

Response: We disagree. These requirements are consistent with U.S. Supreme Court cases holding that warrantless administrative searches of commercial property are not per se violations of the Fourth Amendment. The provisions requiring that covered entities provide access to certain material to determine compliance with the regulation come within the well settled exception regarding closely regulated businesses and industries to the warrant requirement. From state and local licensure laws to the federal fraud and abuse statutes and regulations, the health care industry

1/3/2003

is one of the most [82590 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] tightly regulated businesses in the country. Because the industry has such an extensive history of government oversight and involvement, those operating within it have no reasonable expectation of privacy from the government such that a warrant would be required to determine compliance with the rules. In addition, the cases cited by the commenters concern unannounced searches of the premises and facilities of particular entities. Because our enforcement provisions only provide for the review of books, records, and other information and only during normal business hours with notice, except for exceptional situations, this case law does not apply. As for business associates, they voluntarily enter into their agreements with covered entities. This agreement, therefore, functions as knowing and voluntary consents to the search (even assuming it could be understood to be a search) and obviates the need for a warrant.

Fifth Amendment

Comment: Several comments asserted that the proposed rules violated the Fifth Amendment because in the commenters' views they authorized the taking of privacy property without just compensation or due process of law.

Response: We disagree. The rules set forth below do not address the issue of who owns an individual's medical record. Instead, they address what uses and disclosures of protected health information may be made by covered entities with or without a consent or authorization. As described in response to a similar comment, medical records have been the property of the health care provider or medical facility that created them, historically. In some states, statutes directly provide these entities with ownership. These laws are limited by laws that provide patients or their representatives with access to the records or that provide the patient with an ownership interest in the information within the records. As we discuss, the final rule is consistent with current state law that provides patients access to protected health information, but not ownership of medical records. State laws that provide patients with greater access would remain in effect. Therefore, because patients do not own their records, no taking can occur. As for their interest in the information, the final rule retains their rights. As for covered entities, the final rule does not take away their ownership rights or make their ownership interest in the protected health information worthless. Therefore, no taking has occurred in these situations either.

Ninth and Tenth Amendments

Comment: Several comments asserted that the proposed rules violated the Ninth and Tenth Amendments. One commenter suggested that the Ninth Amendment prohibits long and complicated regulations. Other commenters suggested that the proposed rules authorized the compelled disclosure of individually identifiable health information in violation of State constitutional provisions, such as those in California

1/3/2003

and Florida. Similarly, a couple of commenters asserted that the privacy rules violate the Tenth Amendment.

Response: We disagree. The Ninth and Tenth Amendments address the rights retained by the people and acknowledge that the States or the people are reserved the powers not delegated to the federal government and not otherwise prohibited by the Constitution. Because HHS is regulating under a delegation of authority from Congress in an area that affects interstate commerce, we are within the powers provided to Congress in the Constitution. Nothing in the Ninth Amendment, or any other provision of the Constitution, restricts the length or complexity of any law. Additionally, we do not believe the rules below impermissibly authorize behavior that violates State constitutions. This rule requires disclosure only to the individual or to the Secretary to enforce this rule. As noted in the preamble discussion of “Preemption,” these rules do not preempt State laws, including constitutional provisions, that are contrary to and more stringent, as defined at § 160.502, than these rules. See the discussion of “Preemption” for further clarification. Therefore, if these State constitutions are contrary to the rule below and provide greater protection, they remain in full force; if they do not, they are preempted, in accordance with the Supremacy Clause of the Constitution.

Right to Privacy

Comment: Several comments suggested that the proposed regulation would violate the right to privacy guaranteed by the First, Fourth, Fifth, and Ninth Amendments because it would permit covered entities to disclose protected health information without the consent of the individual.

Response: These comments did not provide specific facts or legal basis for the claims. We are, thus, unable to provide a substantive response to these particular comments. However, we note that the rule requires disclosures only to the individual or to the Secretary to determine compliance with this rule. Other uses or disclosures under this rule are permissive, not required. Therefore, if a particular use or disclosure under this rule is viewed as interfering with a right that prohibited the use or disclosure, the rule itself is not what requires the use or disclosure.

Void for Vagueness

Comment: One comment suggested that the Secretary’s use of a “reasonableness” standard is unconstitutionally vague. Specifically, this comment objected to the requirement that covered entities use “reasonable” efforts to use or disclose the minimum amount of protected health information, to ensure that business partners comply with the privacy provisions of their contracts, to notify business partners of any amendments or corrections to protected health information, and to verify the identity of individuals requesting information, as well as charge only a “reasonable” fee for inspecting and copying health information. This comment asserted that the Secretary provided “inadequate guidance” as to what qualifies as “reasonable.”

1/3/2003

Response: We disagree with the comment's suggestion that by applying a "reasonableness" standard, the regulation has failed to provide for "fair warning" or "fair enforcement." The "reasonableness" standard is well established in law; for example, it is the foundation of the common law of torts. Courts also have consistently held as constitutional statutes that rely upon a "reasonableness" standard. Our reliance upon a "reasonableness" standard, thus, provides covered entities with constitutionally sufficient guidance.

Criminal Intent

Comment: One comment argued that the regulation's reliance upon a "reasonableness" standard criminalizes "unreasonable efforts" without requiring criminal intent or mens rea.

Response: We reject this suggestion because HIPAA clearly provides the criminal intent requirement. Specifically, HIPAA provides that a "person who knowingly and in violation of this part—(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b)." HIPAA section 1177 (emphasis added). Subsection (b) also relies on a knowledge standard in [82591 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] outlining the three levels of criminal sanctions. Thus, Congress, not the Secretary, established the mens rea by including the term "knowingly" in the criminal penalty provisions of HIPAA.

Data Collection

Comment: One commenter suggested that the U.S. Constitution authorized the collection of data on individuals only for the purpose of the census.

Response: While it might be true that the U.S. Constitution expressly discusses the national census, it does not forbid federal agencies from collecting data for other purposes. The ability of agencies to collect non-census data has been upheld by the courts.

Relationship to Other Federal Laws

Comment: We received several comments that sought clarification of the interaction of various federal laws and the privacy regulation. Many of these comments simply listed federal laws and regulations with which the commenter currently must comply. For example, commenters noted that they must comply with regulations relating to safety, public health, and civil rights, including Medicare and Medicaid, the Americans with Disabilities Act, the Family and Medical Leave Act, the Federal Aviation Administration regulations, the Department of Transportation regulations, the Federal Highway Administration regulations, the Occupational Safety and Health

1/3/2003

Administration regulations, and the Environmental Protection Agency regulations, and alcohol and drug free workplace rules. These commenters suggested that the regulation state clearly and unequivocally that uses or disclosures of protected health information for these purposes were permissible. Some suggested modifying the definition of health care operations to include these uses specifically. Another suggestion was to add a section that permitted the transmission of protected health information to employers when reasonably necessary to comply with federal, state, or municipal laws and regulations, or when necessary for public or employee safety and health.

Response: Although we sympathize with entities' needs to evaluate the existing laws with which they must comply in light of the requirements of the final regulation, we are unable to respond substantially to comments that do not pose specific questions. We offer, however, the following guidance: if an covered entity is required to disclose protected health information pursuant to a specific statutory or regulatory scheme, the covered entity generally will be permitted under § 164.512(a) to make these disclosures without a consent or authorization; if, however, a statute or regulation merely suggests a disclosure, the covered entity will need to determine if the disclosure comes within another category of permissible disclosure under §§ 164.510 or 164.512 or, alternatively, if the disclosure would otherwise come within § 164.502. If not, the entity will need to obtain a consent or authorization for the disclosure.

Comment: One commenter sought clarification as to when a disclosure is considered to be "required" by another law versus "permitted" by that law.

Responses: We use these terms according to their common usage. By "required by law," we mean that a covered entity has a legal obligation to disclose the information. For example, if a statute states that a covered entity must report the names of all individuals presenting with gun shot wounds to the emergency room or else be fined \$500 for each violation, a covered entity would be required by law to disclose the protected health information necessary to comply with this mandate. The privacy regulation permits this type of disclosure, but does not require it. Therefore, if a covered entity chose not to comply with the reporting statute it would violate only the reporting statute and not the privacy regulation. On the other hand, if a statute stated that a covered entity may or is permitted to report the names of all individuals presenting with gun shot wounds to the emergency room and, in turn, would receive \$500 for each month it made these reports, a covered entity would not be permitted by § 164.512(a) to disclose the protected health information. Of course, if another permissible provision applied to these facts, the covered entity could make the disclosure under that provision, but it would not be considered to be a disclosure. See discussion under § 164.512(a) below.

Comment: Several commenters suggested that the proposed rule was unnecessarily duplicative of existing regulations for federal programs, such as Medicare, Medicaid, and the Federal Employee Health Benefit Program.

Response: Congress specifically subjected certain federal programs, including Medicare, Medicaid, and the Federal Employee Health Benefit Program to the

1/3/2003

privacy regulation by including them within the definition of “health plan.” Therefore, covered entities subject to requirements of existing federal programs will also have to comply with the privacy regulation.

Comment: One comment asserts that the regulation would not affect current federal requirements if the current requirements are weaker than the requirements of the privacy regulation. This same commenter suggested that current federal requirements will trump both state law and the proposed regulation, even if Medicaid transactions remain wholly intrastate.

Response: We disagree. As noted in our discussion of “Relationship to Other Federal Laws,” each law or regulation will need to be evaluated individually. We similarly disagree with the second assertion made by the commenter. The final rule will preempt state laws only in specific instances. For a more detailed analysis, see the preamble discussion of “Preemption.”

Administrative Subpoenas

Comment: One comment stated that the final rule should not impose new standards on administrative subpoenas that would conflict with existing laws or administrative or judicial rules that establish standards for issuing subpoenas. Nor should the final rule conflict with established standards for the conduct of administrative, civil, or criminal proceedings, including the rules regarding the discovery of evidence. Other comments sought further restrictions on access to protected health information in this context.

Response: Section 164.512(e) below addresses disclosures for judicial and administrative proceedings. The final rules generally do not interfere with these existing processes to the extent an individual served with a subpoena, court order, or other similar process is able to raise objections already available. See the discussion below under § 164.512(e) for a fuller response.

Americans with Disabilities Act

Comment: Several comments discussed the intersection between the proposed Privacy Rule and the Americans with Disabilities Act (“ADA”) and sections 503 and 504 of the Rehabilitation Act of 1973. One comment suggested that the final rule explicitly allows disclosures authorized by the Americans with Disabilities Act without an individual’s authorization, because this law, in the commenter’s view, provides more than adequate protection for the confidentiality of medical records in the employment context. The comment noted that under these laws employers may receive information related to fitness for duty, pre-employment physicals, routine examinations, return to work examinations, examinations following other types of absences, examinations triggered by specific events, changes in [82592 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] circumstances, requests for reasonable accommodations, leave requests, employee wellness programs, and medical monitoring. Other commenters suggested that the

1/3/2003

ADA requires the disclosure of protected health information to employers so that the employee may take advantage of the protections of these laws. They suggested that the final rules clarify that employment may be conditioned on obtaining an authorization for disclosure of protected health information for lawful purposes and provide guidance concerning the interaction of the ADA with the final regulation's requirements. Several commenters wanted clarification that the privacy regulation would not permit employers to request or use protected health information in violation of the ADA.

Response: We disagree with the comment that the final rule should allow disclosures of protected health information authorized by the ADA without the individual's authorization. We learned from the comments that access to and use of protected health information by employers is of particular concern to many people. With regard to employers, we do not have statutory authority to regulate them. Therefore, it is beyond the scope of this regulation to prohibit employers from requesting or obtaining protected health information. Covered entities may disclose protected health information about individuals who are members of an employer's workforce with an authorization. Nothing in the privacy regulation prohibits employers from obtaining that authorization as a condition of employment. We note, however, that employers must comply with other laws that govern them, such as nondiscrimination laws. For example, if an employer receives a request for a reasonable accommodation, the employer may require reasonable documentation about the employee's disability and the functional limitations that require the reasonable accommodation, if the disability and the limitations are not obvious. If the individual provides insufficient documentation and does not provide the missing information in a timely manner after the employer's subsequent request, the employer may require the individual to go to an appropriate health professional of the employer's choice. In this situation, the employee does not authorize the disclosure of information to substantiate the disability and the need for reasonable accommodation, the employer need not provide the accommodation. We agree that this rule does not permit employers to request or use protected health information in violation of the ADA or other antidiscrimination laws.

Appropriations Laws

Comment: One comment suggested that the penalty provisions of HIPAA, if extended to the privacy regulation, would require the Secretary to violate "Appropriations Laws" because the Secretary could be in the position of assessing penalties against her own and other federal agencies in their roles as covered entities. Enforcing penalties on these entities would require the transfer of agency funds to the General Fund.

Response: We disagree. Although we anticipate achieving voluntary compliance and resolving any disputes prior to the actual assessment of penalties, the Department of Justice's Office of Legal Counsel has determined in similar situations that federal

1/3/2003

agencies have authority to assess penalties against other federal agencies and that doing so is not in violation of the Anti-Deficiency Act, 31 U.S.C. 1341.

Balanced Budget Act of 1997

Comment: One comment expressed concern that the regulation would place tremendous burdens on providers already struggling with the effects of the Balanced Budget Act of 1997.

Response: We appreciate the costs covered entities face when complying with other statutory and regulatory requirements, such as the Balanced Budget Act of 1997. However, HHS cannot address the impact of the Balanced Budget Act or other statutes in the context of this regulation.

Comment: Another comment stated that the regulation is in direct conflict with the Balanced Budget Act of 1997 (“BBA”). The comment asserts that the regulation’s compliance date conflicts with the BBA, as well as Generally Acceptable Accounting Principles. According to the comment, covered entities that made capital acquisitions to ensure compliance with the year 2000 (“Y2K”) problem would not be able to account for the full depreciation of these systems until 2005. Because HIPAA requires compliance before that time, the regulation would force premature obsolescence of this equipment because while it is Y2K compliant, it may be HIPAA non-compliant.

Response: This comment raises two distinct issues—(1) the investment in new equipment and (2) the compliance date. With regard to the first issue, we reject the comment’s assertion that the regulation requires covered entities to purchase new information systems or information technology equipment, but realize that some covered entities may need to update their equipment. We have tried to minimize the costs, while responding appropriately to Congress’ mandate for privacy rules. We have dealt with the cost issues in detail in the “Regulatory Impact Analysis” section of this Preamble. With regard to the second issue, Congress, not the Secretary, established the compliance data at section 1175(b) of the Act.

Civil Rights of Institutionalized Persons Act

Comment: A few comments expressed concern that the privacy regulation would inadvertently hinder the Department of Justice Civil Rights Divisions’ investigations under the Civil Rights of Institutionalized Persons Act (“CRIPA”). These comments suggested clearly including civil rights enforcement activities as health care oversight.

Response: We agree with this comment. We do not intend for the privacy rules to hinder CRIPA investigations. Thus, the final rule includes agencies that are authorized by law to “enforce civil rights laws for which health information is relevant” in the definition of “health oversight agency” at § 164.501. Covered entities are permitted to disclose protected health information to health oversight agencies

1/3/2003

under § 164.512(d) without an authorization. Therefore, we do not believe the final rule should hinder the Department of Justice's ability to conduct investigations pursuant to its authority in CRIPA.

Clinical Laboratory Improvement Amendments

Comment: One comment expressed concern that the proposed definition of health care operations did not include activities related to the quality control clinical studies performed by laboratories to demonstrate the quality of patient test results. Because the Clinical Laboratory Improvement Amendments of 1988 ("CLIA") requires these studies that the comment asserted require the use of protected health information, the comment suggested including this specific activity in the definition of "health care operations."

Response: We do not intend for the privacy regulation to impede the ability of laboratories to comply with the requirements of CLIA. Quality control activities come within the definition of "health care operations" in § 164.501 because they come within the meaning of the term "quality assurance activities." To the extent they would not come within health care operations, but [82593 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] are required by CLIA, the privacy regulation permits clinical laboratories that are regulated by CLIA to comply with mandatory uses and disclosures of protected health information pursuant to § 164.512(a).

Comment: One comment stated that the proposed regulation's right of access for inspection and copying provisions were contrary to CLIA in that CLIA permits laboratories to disclose lab test results only to "authorized persons." This comment suggested that the final rule include language adopting this restriction to ensure that patients not obtain laboratory test results before the appropriate health care provider has reviewed and explained those results to the patients. A similar comment stated that the lack of preemption of state laws could create problems for clinical laboratories under CLIA. Specifically, this comment noted that CLIA permits clinical laboratories to perform tests only upon the written or electronic request of, and to provide the results to, an "authorized person." State laws define who is an "authorized person." The comment expressed concern as to whether the regulation would preempt state laws that only permit physicians to receive test results.

Response: We agree that CLIA controls in these cases. Therefore, we have amended the right of access, § 164.524(a), so that a covered entity that is subject to CLIA does not have to provide access to the individual to the extent such access would be prohibited by law. Because of this change, we believe the preemption concern is moot.

Controlled Substance Act

1/3/2003

Comment: One comment expressed concern that the privacy regulation as proposed would restrict the Drug Enforcement Agency's ("the DEA") enforcement of the Controlled Substances Act ("CSA"). The comment suggested including enforcement activities in the definition of "health oversight agency."

Response: In our view, the privacy regulation should not impede the DEA's ability to enforce the CSA. First, to the extent the CSA requires disclosures to the DEA, these disclosures would be permissible under § 164.512(a). Second, some of the DEA's CSA activities come within the exception for health oversight agencies which permits disclosures to health oversight agencies for: Activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections * * * civil, administrative, or criminal proceedings or actions; and other activity necessary for appropriate oversight of the health care system. Therefore, to the extent the DEA is enforcing the CSA, disclosures to it in its capacity as a health oversight agency are permissible under § 164.512(d). Alternatively, CSA required disclosures to the DEA for law enforcement purposes are permitted under § 164.512(f). When acting as a law enforcement agency under the CSA, the DEA may obtain the information pursuant to § 164.512(f). Thus, we do not agree that the privacy regulation will impede the DEA's enforcement of the CSA. See the preamble discussion of § 164.512 for further explanation.

Comment: One commenter suggested clarifying the provisions allowing disclosures that are "required by law" to ensure that the mandatory reporting requirements the CSA imposes on covered entities, including making available reports, inventories, and records of transactions, are not preempted by the regulation.

Response: We agree that the privacy regulation does not alter covered entities' obligations under the CSA. Because the CSA requires covered entities manufacturing, distributing, and/or dispensing controlled substances to maintain and provide to the DEA specific records and reports, the privacy regulation permits these disclosures under § 164.512(a). In addition, when the DEA seeks documents to determine an entity's compliance with the CSA, such disclosures are permitted under § 164.512(d).

Comment: The same commenter expressed concern that the proposed privacy regulation inappropriately limits voluntary reporting and would prevent or deter employees of covered entities from providing the DEA with information about violations of the CSA.

Response: We agree with the general concerns expressed in this comment. We do not believe the privacy rules will limit voluntary reporting of violations of the CSA. The CSA requires certain entities to maintain several types of records that may include protected health information. Although reports that included protected health information may be restricted under these rules, reporting the fact that an entity is not maintaining proper reports is not. If it were necessary to obtain protected health information during the investigatory stages following such a voluntary report, the DEA would be able to obtain the information in other ways, such as by following the administrative procedures outlined in § 164.512(e). We also agree that employees of covered entities who report violations of the CSA should not be subjected to

1/3/2003

retaliation by their employers. Under § 164.502(j), we specifically state that a covered entity is not considered to have violated the regulation if a workforce member or business associate in good faith reports violations of laws or professional standards by covered entities to appropriate authorities. See discussion of § 164.502(j) below.

Department of Transportation

Comment: Several commenters stated that the Secretary should recognize in the preamble that it is permissible for employers to condition employment on an individual's delivering a consent to certain medical tests and/or examinations, such as drug-free workplace programs and Department of Transportation ("DOT")-required physical examinations. These comments also suggested that employers should be able to receive certain information, such as pass/fail test and examination results, fitness-to-work assessments, and other legally required or permissible physical assessments without obtaining an authorization. To achieve this goal, these comments suggested defining "health information" to exclude information such as information about how much weight a specific employee can lift.

Response: We reject the suggestion to define "health information," which Congress defined in HIPAA, so that it excludes individually identifiable health information that may be relevant to employers for these types of examinations and programs. We do not regulate employers. Nothing in the rules prohibit employers from conditioning employment on an individual signing the appropriate consent or authorization. By the same token, however, the rules below do not relieve employers from their obligations under the ADA and other laws that restrict the disclosure of individually identifiable health information.

Comment: One commenter asserted that the proposed regulation conflicts with the DOT guidelines regarding positive alcohol and drug tests that require the employer be notified in writing of the results. This document contains protected health information. In addition, the treatment center records must be provided to the Substance Abuse Professional ("SAP") and the employer must receive a report from SAP with random drug testing recommendations.

Response: It is our understanding that DOT requires drug testing of all applicants for employment in safety sensitive positions or individuals being transferred to such positions. [82594 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] Employers, pursuant to DOT regulations, may condition an employee's employment or position upon first obtaining an authorization for the disclosure of results of these tests to the employer. Therefore, we do not believe the final rules conflict with the DOT requirements, which do not prohibit obtaining authorizations before such information is disclosed to employers.

Developmental Disabilities Act

1/3/2003

Comment: One commenter urged HHS to ensure that the regulation would not impede access to individually identifiable health information to entities that are part of the Protection and Advocacy System to investigate abuse and neglect as authorized by the Developmental Disabilities Bill of Rights Act.

Response: The Developmental

Disabilities Assistance and Bill of Rights Act of 2000 (“DD Act”) mandates specific disclosures of individually identifiable health information to Protection and Advocacy systems designated by the chief elected official of the states and Territories.

Therefore, covered entities may make these disclosures under § 164.512(a) without first obtaining an individual’s authorization, except in those circumstances in which the DD Act requires the individual’s authorization. Therefore, the rules below will not impede the functioning of the existing Protection and Advocacy System. Employee Retirement Income Security Act of 1974

Comment: Several commenters objected to the fact that the NPRM did not clarify the scope of preemption of state laws under the Employee Retirement Income Security Act of 1974 (ERISA). These commenters asserted that the final rule must state that ERISA preempts all state laws (including those relating to the privacy of individually identifiable health information) so that multistate employers could continue to administer their group health plans using a single set of rules. In contrast, other commenters criticized the Department for its analysis of the current principles governing ERISA preemption of state law, pointing out that the Department has no authority to interpret ERISA.

Response: This Department has no authority to issue regulations under ERISA as requested by some of these commenters, so the rule below does not contain the statement requested. See the discussion of this point under “Preemption” above.

Comment: One commenter requested that the final rule clarify that section 264(c)(2) of HIPAA does not save state laws that would otherwise be preempted by the Federal Employees Health Benefits Program. The commenter noted that in the NPRM this statement was made with respect to Medicare and ERISA, but not the law governing the FEHBP.

Response: We agree with this comment. The preemption analysis set out above with respect to ERISA applies equally to the Federal Employees Health Benefit Program.

Comment: One commenter noted that the final rule should clarify the interplay between state law, the preemption standards in Subtitle A of Title I of HIPAA (Health Care Access, Portability and Renewability), and the preemption standards in the privacy requirements in Subtitle F of Title II of HIPAA (Administrative Simplification).

Response: The NPRM described only the preemption standards that apply with respect to the statutory provisions of HIPAA that were implemented by the proposed rule. We agree that the preemption standards in Subtitle A of Title I of HIPAA are different. Congress expressly provided that the preemption provisions of Title I apply only to Part 7, which addresses portability, access, and renewability requirements for Group Health Plans. To the extent state laws contain provisions regarding portability, access, or renewability, as well as privacy requirements, a covered entity will need to evaluate the privacy provisions under the Title II preemption provisions, as explained

1/3/2003

in the preemption provisions of the rules, and the other provisions under the Title I preemption requirements.

*European Union Privacy Directive and
U.S. Safe Harbors*

Comment: Several comments stated that the privacy regulation should be consistent with the European Union's Directive on Data Protection. Others sought guidance as to how to comply with both the E.U. Directive on Data Protection and the U.S. Safe Harbor Privacy Principles.

Response: We appreciate the need for covered entities obtaining personal data from the European Union to understand how the privacy regulation intersects with the Data Protection Directive. We have provided guidance as to this interaction in the "Other Federal Laws" provisions of the preamble.

Comment: A few comments expressed concern that the proposed definition of "individual" excluded foreign military and diplomatic personnel and their dependents, as well as overseas foreign national beneficiaries. They noted that the distinctions are based on nationality and are inconsistent with the stance of the E.U. Directive on Data Protection and the Department of Commerce's assurances to the European Commission.

Response: We agree with the general principle that privacy protections should protect every person, regardless of nationality. As noted in the discussion of the definition of "individual," the final regulation's definition does not exclude foreign military and diplomatic personnel, their dependents, or overseas foreign national beneficiaries from the definition of individual. As described in the discussion of § 164.512 below, the final rule applies to foreign diplomatic personnel and their dependents like all other individuals. Foreign military personnel receive the same treatment under the final rule as U.S. military personnel do, as discussed with regard to § 164.512 below. Overseas foreign national beneficiaries to the extent they receive care for the Department of Defense or a source acting on behalf of the Department of Defense remain generally excluded from the final rules protections. For a more detailed explanation, see § 164.500.

Fair Credit Reporting Act

Comment: A few commenters requested that we exclude information maintained, used, or disclosed pursuant to the Fair Credit Reporting Act ("FCRA") from the requirements of the privacy regulation. These commenters noted that the protection in the privacy regulation duplicate those in the FCRA.

Response: Although we realize that some overlap between FCRA and the privacy rules may exist, we have chosen not to remove information that may come within the purview of FCRA from the scope of our rules because FCRA's focus is not the same as our Congressional mandate to protect individually identifiable health information. To the extent a covered entity seeks to engage in collection activities or other

1/3/2003

payment-related activities, it may do so pursuant to the requirements of this rule related to payment. See discussion of §§ 164.501 and 164.502 below. We understand that some covered entities may be part of, or contain components that are, entities which meet the definition of “consumer reporting agencies.” As such, these entities are subject to the FCRA. As described in the preamble to § 164.504, covered entities must designate what parts of their organizations will be treated as covered entities for the [82595 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] purpose of these privacy rules. The covered entity component will need to comply with these rules, while the components that are consumer reporting agencies will need to comply with FCRA. Comment: One comment suggested that the privacy regulation would conflict with the FCRA if the regulation’s requirement applied to information disclosed to consumer reporting agencies.

Response: To the extent a covered entity is required to disclose protected health information to a consumer reporting agency, it may do so under § 164.512(a). See also discussion under the definition of “payment” below.

Fair Debt Collection and Practices Act

Comment: Several comments expressed concern that health plans and health care providers be able to continue using debt collectors in compliance with the Fair Debt Collections Practices Act and related laws.

Response: In our view, health plans and health care providers will be able to continue using debt collectors. Using the services of a debt collector to obtain payment for the provision of health care comes within the definition of “payment” and is permitted under the regulation. Thus, so long as the use of debt collectors is consistent with the regulatory requirements (such as, providers obtain the proper consents, the disclosure is of the minimum amount of information necessary to collect the debt, the provider or health plan enter into a business associate agreement with the debt collector, etc.), relying upon debt collectors to obtain reimbursement for the provision of health care would not be prohibited by the regulation.

Family Medical Leave Act

Comment: One comment suggested that the proposed regulation adversely affects the ability of an employer to determine an employee’s entitlement to leave under the Family Medical Leave Act (“FMLA”) by affecting the employer’s right to receive medical certification of the need for leave, additional certifications, and fitness for duty certification at the end of the leave. The commenter sought clarification as to whether a provider could disclose information to an employer without first obtaining an individual’s consent or authorization. Another commenter suggested that the final rule explicitly exclude from the rule disclosures authorized by the FMLA, because, in

1/3/2003

the commenter's view, it provides more than adequate protection for the confidentiality of medical records in the employment context.

Response: We disagree that the FMLA provides adequate privacy protections for individually identifiable health information. As we understand the FMLA, the need for employers to obtain protected health information under the statute is analogous to the employer's need for protected health information under the ADA. In both situations, employers may need protected health information to fulfill their obligations under these statutes, but neither statute requires covered entities to provide the information directly to the employer. Thus, covered entities in these circumstances will need an individual's authorizations before the disclosure is made to the employer.

Federal Common Law

Comment: One commenter did not want the privacy rules to interfere with the federal common law governing collective bargaining agreements permitting employers to insist on the cooperation of employees with medical fitness evaluations.

Response: We do not seek to interfere with legal medical fitness evaluations. These rules require a covered entity to have an individual's authorization before the information resulting from such evaluations is disclosed to the employer unless another provision of the rule applies. We do not prohibit employers from conditioning employment, accommodations, or other benefits, when legally permitted to do so, upon the individual/employee providing an authorization that would permit the disclosure of protected health information to employers by covered entities. See § 164.508(b)(4) below.

Federal Educational Rights and Privacy Act

Comment: A few commenters supported the exclusion of "education records" from the definition of "protected health information." However, one commenter requested that "treatment records" of students who are 18 years or older attending postsecondary education institutions be excluded from the definition of "protected health information" as well to avoid confusion.

Response: We agree with these commenters. See "Relationship to Other Federal Laws" for a description of our exclusion of FERPA "education records" and records defined at 20 U.S.C. 1232g(a)(4)(B)(iv), commonly referred to as "treatment records," from the definition of "protected health information."

Comment: One comment suggested that the regulation should not apply to any health information that is part of an "education record" in any educational agency or institution, regardless of its FERPA status.

Response: We disagree. As noted in our discussion of "Relationship of Other Federal Laws," we exclude education records from the definition of protected health

1/3/2003

information because Congress expressly provided privacy protections for these records and explained how these records should be treated in FERPA.

Comment: One commenter suggested eliminating the preamble language that describes school nurses and on-site clinics as acting as providers and subject to the privacy regulation, noting that this language is confusing and inconsistent with the statements provided in the preamble explicitly stating that HIPAA does not preempt FERPA.

Response: We agree that this language may have been confusing. We have provided a clearer expression of when schools may be required to comply with the privacy regulation in the “Relationship to Other Federal Laws” section of the preamble.

Comment: One commenter suggested adding a discussion of FERPA to the “Relationship to Other Federal Laws” section of the preamble.

Response: We agree and have added FERPA to the list of federal laws discussed in “Relationship to Other Federal Laws” section of the preamble.

Comment: One commenter stated that school clinics should not have to comply with the “ancillary” administrative requirements, such as designating a privacy official, maintaining documentation of their policies and procedures, and providing the Secretary of HHS with access.

Response: We disagree. Because we have excluded education records and records described at 20 U.S.C. 1232g(a)(4)(B)(iv) held by educational agencies and institutions subject to FERPA from the definition of protected health information, only non-FERPA schools would be subject to the administrative requirements. Most of these school clinics will also not be covered entities because they are not engaged in HIPAA transactions and these administrative requirements will not apply to them. However, to the extent a school clinic is within the definition of a health care provider, as Congress defined the term, and the school clinic is engaged in HIPAA transactions, it will be a covered entity and must comply with the rules below.

Comment: Several commenters expressed concern that the privacy regulation would eliminate the parents’ ability to have access to information in their children’s school health records. Because the proposed regulation suggests that school-based clinics keep health records separate from other educational files, these comments argued that the regulation is contrary to the spirit of FERPA, which provides parents with access rights to their children’s educational files.

Response: As noted in the “Relationship to Other Federal Laws” provision of the preamble, to the extent information in school-based clinics is not protected health information because it is an education record, the FERPA access requirements apply and this regulation does not. For more detail regarding the rule’s application to unemancipated minors, see the preamble discussion about “Personal Representatives.”

Federal Employees Compensation Act

1/3/2003

Comment: One comment noted that the Federal Employees Compensation Act (“FECA”) requires claimants to sign a release form when they file a claim. This commenter suggested that the privacy regulation should not place additional restrictions on this type of release form.

Response: We agree. In the final rule, we have added a new provision, § 164.512(l), that permits covered entities to make disclosures authorized under workers’ compensation and similar laws. This provision would permit covered entities to make disclosures authorized under FECA and not require a different release form.

Federal Employees Health Benefits Program

Comment: A few comments expressed concern about the preemption effect on FEHBP and wanted clarification that the privacy regulation does not alter the existing preemptive scope of the program.

Response: We do not intend to affect the preemptive scope of the FEHBP. The Federal Employee Health Benefit Act of 1998 preempts any state law that “relates to” health insurance or plans. 5 U.S.C. 8902(m). The final rule does not attempt to alter the preemptive scope Congress has provided to the FEHBP.

Comment: One comment suggested that in the context of FEHBP HHS should place the enforcement responsibilities of the privacy regulation with Office of Personnel Management, as the agency responsible for administering the program.

Response: We disagree. Congress placed enforcement with the Secretary. See section 1176 of the Act.

Federal Rules of Civil Procedure

Comment: A few comments suggested revising proposed § 164.510(d) so that it is consistent with the existing discovery procedure under the Federal Rules of Civil Procedure or local rules.

Response: We disagree that the rules regarding disclosures and uses of protected health information for judicial and administrative procedures should provide only those protections that exist under existing discovery rules. Although the current process may be appropriate for other documents and information requested during the discovery process, the current system, as exemplified by the Federal Rules of Civil Procedure, does not provide sufficient protection for protected health information. Under current discovery rules, private attorneys, government officials, and others who develop such requests make the initial determinations as to what information or documentation should be disclosed. Independent third-party review, such as that by a court, only becomes necessary if a person of whom the request is made refuses to provide the information. If this happens, the person seeking discovery must obtain a court order or move to compel discovery. In our view this system does not provide sufficient protections to ensure that unnecessary and unwarranted disclosures of protected health information does not occur. For a

1/3/2003

related discuss, see the preamble regarding “Disclosures for Judicial and Administrative Proceedings” under § 164.512(e).

Federal Rules of Evidence

Comment: Many comments requested clarification that the privacy regulation does not conflict or interfere with the federal or state privileges. In particular, one of these comments suggested that the final regulation provide that disclosures for a purpose recognized by the regulation not constitute a waiver of federal or state privileges.

Response: We do not intend for the privacy regulation to interfere with federal or state rules of evidence that create privileges. Consistent with The Uniform Health-Care Information Act drafted by the National Conference of Commissioners on Uniform State Laws, we do not view a consent or an authorization to function as a waiver of federal or state privileges. For further discussion of the effect of consent or authorization on federal or state privileges, see preamble discussions in §§ 164.506 and 164.508.

Comment: Other comments applauded the Secretary’s references to *Jaffee v. Redman*, 518 U.S. 1 (1996), which recognized a psychotherapist patient privilege, and asked the Secretary to incorporate expressly this privilege into the final regulation.

Response: We agree that the psychotherapist-patient relationship is an important one that deserves protection. However, it is beyond the scope our mandate to create specific evidentiary privileges. It is also unnecessary because the United States Supreme Court has adopted this privilege.

Comment: A few comments discussed whether one remedy for violating the privacy regulation should be to exclude or suppress evidence obtained in violation of the regulation. One comment supported using this penalty, while another opposed it.

Response: We do not have the authority to mandate that courts apply or not apply the exclusionary rule to evidence obtained in violation of the regulation. This issue is in the purview of the courts.

Federal Tort Claims Act

Comment: One comment contended that the proposed regulation’s requirement mandating covered entities to name the subjects of protected health information disclosed under a business partner contract as third party intended beneficiaries under the contract would have created an impermissible right of action against the government under the Federal Tort Claims Act (“FTCA”).

Response: Because we have deleted the third party beneficiary provisions from the final rules, this comment is moot.

Comment: Another comment suggested the regulation would hamper the ability of federal agencies to disclose protected health information to their attorneys, the Department of Justice, during the initial stages of the claims brought under the FTCA.

1/3/2003

Response: We disagree. The regulation applies only to federal agencies that are covered entities. To the extent an agency is not a covered entity, it is not subject to the regulation; to the extent an agency is a covered entity, it must comply with the regulation. A covered entity that is a federal agency may disclose relevant information to its attorneys, who are business associates, for purposes of health care operations, which includes uses or disclosures for legal functions. See § 164.501 (definitions of “business associate” and “health care operations”). The final rule provides specific provisions describing how federal agencies may provide [82597 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] adequate assurances for these types of disclosures of protected health information. See § 164.504(e)(3).

Food and Drug Administration

Comment: A few comments expressed concerns about the use of protected health information for reporting activities to the Food and Drug Administration (“FDA”). Their concern focused on the ability to obtain or disclose protected health information for pre-and post-marketing adverse event reports, device tracking, and postmarketing safety and efficacy evaluation.

Response: We agree with this comment and have provided that covered entities may disclose protected health information to persons subject to the jurisdiction of the FDA, to comply with the requirements of, or at the direction of, the FDA with regard to reporting adverse events (or similar reports with respect to dietary supplements), the tracking of medical devices, other post-marketing surveillance, or other similar requirements described at § 164.512(b).

Foreign Standards

Comment: One comment asked how the regulation could be enforced against foreign countries (or presumably entities in foreign countries) that solicit medical records from entities in the United States.

Response: We do not regulate solicitations of information. To the extent a covered entity wants to comply with a request for disclosure of protected health information to foreign countries or entities within foreign countries, it will need to comply with the privacy rules before making the disclosure. If the covered entity fails to comply with the rules, it will be subject to enforcement proceedings.

Freedom of Information Act

Comment: One comment asserted that the proposed privacy regulation conflicts with the Freedom of Information Act (“FOIA”). The comment argued that the proposed restriction on disclosures by agencies would not come within one of the permissible exemptions to the FOIA. In addition, the comment noted that only in exceptional circumstances would the protected health information of deceased individuals come

1/3/2003

within an exemption because, for the most part, death extinguishes an individual's right to privacy.

Response: Section 164.512(a) below permits covered entities to disclose protected health information when such disclosures are required by other laws as long as they follow the requirements of those laws. Therefore, the privacy regulation will not interfere with the ability of federal agencies to comply with FOIA, when it requires the disclosure. We disagree, however, that most protected health information will not come within Exemption 6 of FOIA. See the discussion above under "Relationship to Other Federal Laws" for our review of FOIA. Moreover, we disagree with the comment's assertion that the protected health information of deceased individuals does not come within Exemption 6. Courts have recognized that a deceased individual's surviving relatives may have a privacy interest that federal agencies may consider when balancing privacy interests against the public interest in disclosure of the requested information. Federal agencies will need to consider not only the privacy interests of the subject of the protected health information in the record requested, but also, when appropriate, those of a deceased individual's family consistent with judicial rulings. If an agency receives a FOIA request for the disclosure of protected health information of a deceased individual, it will need to determine whether or not the disclosure comes within Exemption 6. This evaluation must be consistent with the court's rulings in this area. If the exemption applies, the federal agency will not have to release the information. If the federal agency determines that the exemption does not apply, may release it under § 164.512(a) of this regulation.

Comment: One commenter expressed concern that our proposal to protect the individually identifiable health information about the deceased for two years following death would impede public interest reporting and would be at odds with many state Freedom of Information laws that make death records and autopsy reports public information. The commenter suggested permitting medical information to be available upon the death of an individual or, at the very least, that an appeals process be permitted so that health information trustees would be allowed to balance the interests in privacy and in public disclosure and release or not release the information accordingly.

Response: These rules permit covered entities to make disclosures that are required by state Freedom of Information Act (FOIA) laws under § 164.512(a). Thus, if a state FOIA law designates death records and autopsy reports as public information that must be disclosed, a covered entity may disclose it without an authorization under the rule. To the extent that such information is required to be disclosed by FOIA or other law, such disclosures are permitted under the final rule. In addition, to the extent that death records and autopsy reports are obtainable from non-covered entities, such as state legal authorities, access to this information is not impeded by this rule. If another law does not require the disclosure of death records and autopsy reports generated and maintained by a covered entity, which are protected health information, covered entities are not allowed to disclose such information except as permitted or required by the final rule, even if another entity discloses them.

1/3/2003

Comment: One comment sought clarification of the relationship between the Freedom of Information Act, the Privacy Act, and the privacy rules.

Response: We have provided this analysis in the “Relationship to Other Federal Laws” section of the preamble in our discussion of the Freedom of Information Act.

Gramm-Leach-Bliley

Comments: One commenter noted that the Financial Services Modernization Act, also known as Gramm-Leach-Bliley (“GLB”), requires financial institutions to provide detailed privacy notices to individuals. The commenter suggested that the privacy regulation should not require financial institutions to provide additional notice.

Response: We disagree. To the extent a covered entity is required to comply with the notice requirements of GLB and those of our rules, the covered entity must comply with both. We will work with the FTC and other agencies implementing GLB to avoid unnecessary duplication. For a more detailed discussion of GLB and the privacy rules, see the “Relationship to Other Federal Laws” section of the preamble.

Comment: A few commenters asked that the Department clarify that financial institutions, such as banks, that serve as payors are covered entities. The comments explained that with the enactment of the Gramm-Leach-Bliley Act, banks are able to form holding companies that will include insurance companies (that may be covered entities). They recommended that banks be held to the rule’s requirements and be required to obtain authorization to conduct non-payment activities, such as for the marketing of health and nonhealth items and services or the use and disclosure to non-health related divisions of the covered entity. [82598 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

Response: These comments did not provide specific facts that would permit us to provide a substantive response. An organization will need to determine whether it comes within the definition of “covered entity.” An organization may also need to consider whether or not it contains a health care component. Organizations that are uncertain about the application of the regulation to them will need to evaluate their specific facts in light of this rule.

Inspector General Act

Comment: One comment requested the Secretary to clarify in the preamble that the privacy regulation does not preempt the Inspector General Act.

Response: We agree that to the extent the Inspector General Act requires uses or disclosures of protected health information, the privacy regulation does not preempt it. The final rule provides that to the extent required under section 201(a)(5) of the Act, nothing in this subchapter should be construed to diminish the authority of any Inspector General, including the authority provided in the Inspector General Act of 1978. See discussion of § 160.102 above.

1/3/2003

Medicare and Medicaid

Comment: One comment suggested possible inconsistencies between the regulation and Medicare/Medicaid requirements, such as those under the Quality Improvement System for Managed Care. This commenter asked that HHS expand the definition of health care operations to include health promotion activities and avoid potential conflicts.

Response: We disagree that the privacy regulation would prohibit managed care plans operating in the Medicare or Medicaid programs from fulfilling their statutory obligations. To the extent a covered entity is required by law to use or disclose protected health information in a particular manner, the covered entity may make such a use or disclosure under § 164.512(a). Additionally, quality assessment and improvement activities come within the definition of “health care operations.” Therefore, the specific example provided by the commenter would seem to be a permissible use or disclosure under § 164.502, even if it were not a use or disclosure “required by law.”

Comment: One commenter stated that Medicare should not be able to require the disclosure of psychotherapy notes because it would destroy a practitioner’s ability to treat patients effectively.

Response: If the Title XVIII of the Social Security Act requires the disclosure of psychotherapy notes, the final rule permits, but does not require, a covered entity to make such a disclosure under § 164.512(a). If, however, the Social Security Act does not require such disclosures, Medicare does not have the discretion to require the disclosure of psychotherapy notes as a public policy matter because the final rule provides that covered entities, with limited exceptions, must obtain an individual’s authorization before disclosing psychotherapy notes. See § 164.508(a)(2).

National Labor Relations Act

Comment: A few comments expressed concern that the regulation did not address the obligation of covered entities to disclose protected health information to collective bargaining representatives under the National Labor Relations Act.

Response: The final rule does not prohibit disclosures that covered entities must make pursuant to other laws. To the extent a covered entity is required by law to disclose protected health information to collective bargaining representatives under the NLRA, it may do so without an authorization. Also, the definition of “health care operations” at § 164.501 permits disclosures to employee representatives for purposes of grievance resolution.

Organ Donation

Comment: One commenter expressed concern about the potential impact of the regulation on the organ donation program under 42 CFR part 482.

1/3/2003

Response: In the final rule, we add provisions allowing the use or disclosure of protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating donation and transplantation. See § 164.512(h).

Privacy Act Comments

Comment: One comment suggested that the final rule unambiguously permit the continued operation of the statutorily established or authorized discretionary routine uses permitted under the Privacy Act for both law enforcement and health oversight.

Response: We disagree. See the discussion of the Privacy Act in “Relationship to Other Federal Laws” above.

Public Health Services Act

Comment: One comment suggested that the Public Health Service Act places more stringent rules regarding the disclosure of information on Federally Qualified Health Centers than the proposed privacy regulation suggested. Therefore, the commenter suggested that the final rule exempt Federally Qualified Health Centers from the rules requirements.

Response: We disagree. Congress expressly included Federally Qualified Health Centers, a provider of medical or other health services under the Social Security Act section 1861(s), within its definition of health care provider in section 1171 of the Act; therefore, we cannot exclude them from the regulation.

Comment: One commenter noted that no conflicts existed between the proposed rule and the Public Health Services Act.

Response: As we discuss in the “Relationship to Other Federal Laws” section of the preamble, the Public Health Service Act contains explicit confidentiality requirements that are so general as not to create problems of inconsistency. We recognized, however, that in some cases, that law or its accompanying regulations may contain greater restrictions. In those situations, a covered entity’s ability to make what are permissive disclosures under this privacy regulation would be limited by those laws.

Reporting Requirement

Comment: One comment noted that federal agencies must provide information to certain entities pursuant to various federal statutes. For example, federal agencies must not withhold information from a Congressional oversight committee or the General Accounting Office. Similarly, some federal agencies must provide the Bureau of the Census and the National Archives and Records Administration with certain information. This comment expressed concern that the privacy regulation would conflict with these requirements. Additionally, the commenter asked whether the privacy notice would need to contain these uses and disclosures and

1/3/2003

recommended that a general statement that these federal agencies would disclose protected health information when required by law be considered sufficient to meet the privacy notice requirements.

Response: To the extent a federal agency acting as a covered entity is required by federal statute to disclose protected health information, the regulation permits the disclosure as required by law under § 164.512(a). The notice provisions at § 164.520(b)(1)(ii)(B) require covered entities to provide a brief description of the purposes for which the covered [82599 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] entity is permitted or required by the rules to use or disclose protected health information without an individual's written authorization. If these statutes require the disclosures, covered entities subject to the requirement may make the disclosure pursuant to § 164.512(a). Thus, their notice must include a description of the category of these disclosures. For example, a general statement such as the covered entity "will disclose your protected health information to comply with legal requirements" should suffice.

Comment: One comment stressed that the final rule should not inadvertently preempt mandatory reporting laws duly enacted by federal, state, or local legislative bodies. This commenter also suggested that the final rule not prevent the reporting of violations to law enforcement agencies.

Response: We agree. Like the proposed rule, the final rule permits covered entities to disclose protected health information when required by law under § 164.512(a). To the extent a covered entity is required by law to make a report to law enforcement agencies or is otherwise permitted to make a disclosure to a law enforcement agency as described in § 164.512(f), it may do so without an authorization. Alternatively, a covered entity may always request that individuals authorize these disclosures.

Security Standards

Comment: One comment called for HHS to consider the privacy regulation in conjunction with the other HIPAA standards. In particular, this comment focused on the belief that the security standards should be compatible with the existing and emerging health care and information technology industry standards.

Response: We agree that the security standards and the privacy rules should be compatible with one another and are working to ensure that the final rules in both areas function together. Because we are addressing comments regarding the privacy rules in this preamble, we will consider the comment about the security standard as we finalize that set of rules.

Substance Abuse Confidentiality Statute and Regulations

1/3/2003

Comment: Several commenters noted that many health care providers are bound by the federal restrictions governing alcohol and drug abuse records. One commenter noted that the NPRM differed substantially from the substance abuse regulations and would have caused a host of practical problems for covered entities. Another commenter, however, supported the NPRM's analysis that stated that more stringent provisions of the substance abuse provisions would apply. This commenter suggested an even stronger approach of including in the text a provision that would preserve existing federal law. Yet, one comment suggested that the regulation as proposed would confuse providers by making it difficult to determine when they may disclose information to law enforcement because the privacy regulation would permit disclosures that the substance abuse regulations would not.

Response: We appreciate the need of some covered entities to evaluate the privacy rules in light of federal requirements regarding alcohol and drug abuse records. Therefore, we provide a more detailed analysis in the "Relationship to Other Federal Laws" section of the preamble.

Comment: Some of these commenters also noted that state laws contain strict confidentiality requirements. A few commenters suggested that HHS reassess the regulations to avoid inconsistencies with state privacy requirements, implying that problems exist because of conflicts between the federal and state laws regarding the confidentiality of substance abuse information.

Response: As noted in the preamble section discussing preemption, the final rules do not preempt state laws that provide more privacy protections. For a more detailed analysis of the relationship between state law and the privacy rules, see the "Preemption" provisions of the preamble.

Tribal Law

Comments: One commenter suggested that the consultation process with tribal governments described in the NPRM was inadequate under Executive Order No. 13084. In addition, the commenter expressed concern that the disclosures for research purposes as permitted by the NPRM would conflict with a number of tribal laws that offer individuals greater privacy rights with respect to research and reflects cultural appropriateness. In particular, the commenter referenced the Health Research Code for the Navajo Nation which creates a entity with broader authority over research conducted on the Navajo Nation than the local IRB and requires informed consent by study participants. Other laws mentioned by the commenter included the Navajo Nation Privacy and Access to Information Act and a similar policy applicable to all health care providers within the Navajo Nation. The commenter expressed concern that the proposed regulation research provisions would override these tribal laws.

Response: We disagree with the comment that the consultation with tribal governments undertaken prior to the proposed regulation is inadequate under Executive Order No. 13084. As stated in the proposed regulation, the Department consulted with representatives of the National Congress of American Indians and the

1/3/2003

National Indian Health Board, as well as others, about the proposals and the application of HIPAA to the Tribes, and the potential variations based on the relationship of each Tribe with the HIS for the purpose of providing health services. In addition, Indian and tribal governments had the opportunity to, and did, submit substantive comments on the proposed rules. Additionally, disclosures permitted by this regulation do not conflict with the policies as described by this commenter. Disclosures for research purposes under the final rule, as in the proposed regulation, are permissive disclosures only. The rule describes the outer boundaries of permissible disclosures. A covered health care provider that is subject to the tribal laws of the Navajo Nation must continue to comply with those tribal laws. If the tribal laws impose more stringent privacy standards on disclosures for research, such as requiring informed consent in all cases, nothing in the final rule would preclude compliance with those more stringent privacy standards. The final rule does not interfere with the internal governance of the Navajo Nation or otherwise adversely affect the policy choices of the tribal government with respect to the cultural appropriateness of research conducted in the Navajo Nation.

TRICARE

Comment: One comment expressed concern regarding the application of the “minimum necessary” standard to investigations of health care providers under the TRICARE (formerly the CHAMPUS) program. The comment also expressed concern that health care providers would be able to avoid providing their records to such investigators because the proposed § 164.510 exceptions were not mandatory disclosures.

Response: In our view, neither the minimum necessary standard nor the final §§ 164.510 and 164.512 permissive disclosures will impede such investigations. The regulation requires covered entities to make all reasonable efforts not to disclose more than the minimum amount of protected health [82600 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] information necessary to accomplish the intended purpose of the use or disclosure. This requirement, however, does not apply to uses or disclosures that are required by law. See § 164.502(b)(2)(iv). Thus, if the disclosure to the investigators is required by law, the minimum necessary standard will not apply. Additionally, the final rule provides that covered entities rely, if such reliance is reasonable, on assertions from public officials about what information is reasonably necessary for the purpose for which it is being sought. See § 164.514(d)(3)(iii). We disagree with the assertion that providers will be able to avoid providing their records to investigators. Nothing in this rule permits covered entities to avoid disclosures required by other laws.

Veterans Affairs

1/3/2003

Comment: One comment sought clarification about how disclosures of protected health information would occur within the Veterans Affairs programs for veterans and their dependents.

Response: We appreciate the commenter's request for clarification as to how the rules will affect disclosures of protected health information in the specific context of Veteran's Affairs programs. Veterans health care programs under 38 U.S.C. chapter 17 are defined as "health plans." Without sufficient details as to the particular aspects of the Veterans Affairs programs that this comment views as problematic, we cannot comment substantively on this concern.

Comment: One comment suggested that the final regulation clarify that the analysis applied to the substance abuse regulations apply to laws governing Veteran's Affairs health records.

Response: Although we realize some difference may exist between the laws, we believe the discussion of federal substance abuse confidentiality regulations in the "Relationship to Other Federal Laws" preamble provides guidance that may be applied to the laws governing Veteran's Affairs ("VA") health records. In most cases, a conflict will not exist between these privacy rules and the VA programs. For example, some disclosures allowed without patient consent or authorization under the privacy regulation may not be within the VA statutory list of permissible disclosures without a written consent. In such circumstances, the covered entity would have to abide by the VA statute, and no conflict exists. If the disclosures permitted by the VA statute come within the permissible disclosures of our rules, no conflict exists. In some cases, our rules may demand additional requirements, such as obtaining the approval of a privacy board or Institutional Review Board if a covered entity seeks to disclose protected health information for research purposes without the individual's authorization. A covered entity subject to the VA statute will need to ensure that it meets the requirements of both that statute and the regulation below. If a conflict arises, the covered entity should evaluate the specific potential conflicting provisions under the implied repeal analysis set forth in the "Relationship to Other Federal Laws" discussion in the preamble.

WIC

Comment: One comment called on other federal agencies to examine their regulations and policies regarding the use and disclosure of protected health information. The comment suggested that other agencies revise their regulations and policies to avoid duplicative, contradictory, or more stringent requirements. The comment noted that the U.S. Department of Agriculture's Special Supplemental Nutrition Program for Women, Infants, and Children ("WIC") does not release WIC data. Because the commenter believed the regulation would not prohibit the disclosure of WIC data, the comment stated that the Department of Agriculture should now release such information.

Response: We support other federal agencies to whom the rules apply in their efforts to review existing regulations and policies regarding protected health information.

1/3/2003

However, we do not agree with the suggestion that other federal agencies that are not covered entities must reduce the protections or access-related rights they provide for individually identifiable health information they hold.

...

Section 164.534—Effective Date and Compliance Date

Compliance Gap Vis-a`-Vis State Laws and Small Health Plans

Comment: Several comments stated that, as drafted, the preemption provisions would be effective as of the rule's effective date (i.e., 60 days following publication), even though covered entities would not be required to comply with the rules for at least another two years. According to these comments, the "preempted" state laws would not be in effect in the interim, so that the actual privacy protection would decrease during that period. A couple of comments also expressed concern about how the preemption provisions would work, given the one-year difference in applicable compliance dates for small health plans and other covered entities. A state medical society pointed out that this gap would also be very troublesome for providers who deal with both "small health plans" and other health plans. One comment asked what entities that decided to come into compliance early would have to do with respect to conflicting state laws and suggested that, since all parties "need to know with confidence which laws govern at the moment, * * * [t]here should be uniform effective dates."

Response: We agree that clarification is needed with respect to the applicability of state laws in the interim between the effective date and the compliance dates. What the comments summarized above appeared to assume is that the preemption provisions of section 1178 operate too broadly and generally invalidate any state law that comes within their ambit. We do not agree that this is the effect of section [82752 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] 1178. Rather, what section 1178 does—where it acts to preempt—is to preempt the state law in question with respect to the actions of covered entities to which the state law applies. Thus, if a provision of state law is preempted by section 1178, covered entities within that state to which the state law applies do not have to comply with it, and must instead comply with the contrary federal standard, requirement, or implementation specification. However, as compliance with the contrary federal standard, requirement, or implementation specification is not required until the applicable compliance date, we do not view the state law in question as meeting the test of being "contrary." That is, since compliance with the federal standard, requirement, or implementation standard is not required prior to the applicable compliance date, it is possible for covered entities to comply with the state law in question. See § 160.202 (definition of "contrary"). Thus, since the state law is

1/3/2003

not “contrary” to an applicable federal standard, requirement, or implementation specification in the period before which compliance is required, it is not preempted. Several implications of this analysis should be spelled out. First, one conclusion that flows from this analysis is that preemption is specific to covered entities and does not represent a general invalidation of state law, as suggested by many commenters. Second, because preemption is covered entity-specific, preemption will occur at different times for small health plans than it will occur for all other covered entities. That is, the preemption of a given state law for a covered entity, such as a provider, that is covered by the 24-month compliance date of section 1175(b)(1)(A) will occur 12 months earlier than the preemption of the same state law for a small health plan that is covered by the 36-month compliance date of section 1175(b)(1)(B). Third, the preemption occurs only for covered entities; a state law that is preempted under section 1178(a)(1) would not be preempted for persons and entities to which it applies who are not covered entities. Thus, to the extent covered entities or noncovered entities follow the federal standards on a voluntary basis (i.e., the covered entity prior to the applicable compliance date, the non-covered entity at any time), the state law in question will not be preempted for them. proposed rules, applauded the decision to extend the compliance date to three years for small businesses. It was requested that the final rules clarify that the three year compliance date applies to small doctors offices and other small entities, as well as to small health plans. Response: We recognize that our discussion in the preamble to the proposed rules may have suggested that more covered entities came within the 36 month compliance date than is in fact the case. Again, this is an area in which we are limited by statute. Under section 1175(b) of the Act, only small health plans have three years to come into compliance with the standards below. Thus, other “small businesses” that are covered entities must comply by the two-year compliance date.

...

IV. Final Regulatory Impact Analysis

...

D. Baseline Privacy Protections

2. State Laws

The second body of privacy protections is found in a complex, and often confusing, myriad of state laws and requirements. To determine whether or not the final rule would preempt a state law, first we identified the relevant laws, and second, we addressed whether state or federal law provides individuals with greater privacy protection. Identifying the Relevant State Statutes: Health information privacy provisions can be found in laws applicable to many issues including insurance,

1/3/2003

worker's compensation, public health, birth and death records, adoptions, education, and welfare. In many cases, state laws were enacted to address a specific situation, such as the reporting of HIV/AIDS, or medical conditions that would impair a person's ability to drive a car. For example, Florida has over 60 laws that apply to protected health information. According to the Georgetown Privacy Project, [fn 39] Florida is not unique. Every state has laws and regulations covering some aspect of medical information privacy. For the purpose of this analysis, we simply acknowledge the variation in state requirements. We recognize that covered entities will need to learn the laws of their states in order to comply with such laws that are not contrary to the rule, or that are contrary to and more stringent than the rule. This analysis should be completed in the context of individual markets; therefore, we expect that professional associations or individual businesses will complete this task. Recognizing the limits of our ability to effectively summarize state privacy laws, we discuss conclusions generated by the Georgetown University Privacy Project's report, *The State of Health Privacy: An Uneven Terrain*. The Georgetown report is among the most comprehensive examination of state health privacy laws currently published, although it is not exhaustive. The report, which was completed in July 1999, is based on a 50-state survey. To facilitate discussion, we have organized the analysis into two sections: access to health information and disclosure of health information. Our analysis is intended to suggest areas where the final rule appears to preempt various state laws; it is not designed to be a definitive or wholly comprehensive state-by-state comparison.

Access to Subject's Information: In general, state statutes provide individuals with some access to medical records about them. However, only a few states allow individuals access to health information held by all their health care providers and health plans. In 33 states, individuals may access their hospital and health facility records. Only 13 states guarantee individuals access to their HMO records, and 16 states provide individuals access to their medical information when it is held by insurers. Seven states have no statutory right of patient access; three states and the District of Columbia have laws that only assure individuals' right to access their mental health records. Only one state permits individuals access to records about them held by health care providers, but it excludes pharmacists from the definition of provider. Thirteen states grant individuals statutory right of access to pharmacy records. The amount that entities are allowed to charge for copying of individuals' records varies widely from state to state. A study conducted by the American Health Information Management Association 40 found considerable variation in the amounts, structure, and combination of fees for search and retrieval, and the copying of the record. In 35 states, there are laws or regulations that set a basis for charging individuals inspecting and copying fees. Charges vary not only by state, but also by the purpose of the request and the facility holding the health information. Also, charges vary by the number of pages and whether the request is for Xrays or for standard medical information. Of the 35 states with laws regulating inspection and copying charges, seven states either do not allow charges for retrieval of records or require that the entity provide the first copy free of charge. Some states

1/3/2003

may prohibit hospitals from charging patients a retrieval and copying fee, but allow clinics to do so. Many states allow fee structures, while eleven states specify only that the record holder may charge “reasonable/actual costs.” According to the report by the Georgetown Privacy Project, among states that do grant access to patient records, the most common basis for denying individuals access is concern for the life and safety of the individual or others. The amount of time an entity is given to supply the individual with his or her record varies widely. Many states allow individuals to amend or correct inaccurate health information, especially information held by insurers. However, few states provide the right to insert a statement in the record challenging the covered entity’s information when the individual and entity disagree. [fn 41]

Disclosure of Health Information: State laws vary widely with respect to disclosure of individually identifiable health information. Generally, states have applied restrictions on the disclosure of health information either to specific entities or for specific health conditions. Only three state laws place broad limits on disclosure of individually identifiable health information without regard for policies and procedures developed by covered entities. Most states require patient authorization before an entity may disclose health information to certain recipients, but the patient often does not have an opportunity to object to any disclosures. [Fn 42] It is also important to point out that none of the states appear to offer individuals the right to restrict disclosure of their health information for treatment [82765 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] [Fn 43] “Medical records and privacy: Empirical effects of legislation; A memorial to Alice Hersch”; McCarthy, Douglas B; Shatin, Deborah; et al. Health Service Research: April 1, 1999; No. 1, Vol. 34; p. 417. The article details the effects of the Minnesota law conditioning disclosure of protected health information on patient authorization. 44 Source Book of Health Insurance Data: 1997– 1998, Health Insurance Association of America, 1998. p. 33. 45 “Health plans,” for purposes of the regulatory impact and regulatory flexibility analyses, include licensed insurance carriers who sell health products; third party administrators that will have to comply with the regulation for the benefit of the plan sponsor; and self-insured health plans that are at least partially administered by the plan sponsor. State statutes often have exceptions to requiring authorization before disclosure. The most common exceptions are for purposes of treatment, payment, or auditing and quality assurance functions. Restrictions on re-disclosure of individually identifiable health information also vary widely from state to state. Some states restrict the re-disclosure of health information, and others do not. The Georgetown report cites state laws that require providers to adhere to professional codes of conduct and ethics with respect to disclosure and redisclosure of protected health information. Most states have adopted specific measures to provide additional protections for health information regarding certain sensitive conditions or illnesses. The conditions and illnesses most commonly afforded added privacy protection are:

- Information derived from genetic testing;
- Communicable and sexually transmitted diseases;
- Mental health; and

1/3/2003

- Abuse, neglect, domestic violence, and sexual assault.

Some states place restrictions on releasing condition-specific health information for research purposes, while others allow release of information for research without the patient's authorization. States frequently require that researchers studying genetic diseases, HIV/AIDS, and other sexually transmitted diseases have different authorization and privacy controls than those used for other types of research. Some states require approval from an IRB or agreements that the data will be destroyed or identifiers removed at the earliest possible time. Another approach has been for states to require researchers to obtain sensitive, identifiable information from a state public health department. One state does not allow automatic release of protected health information for research purposes without notifying the subjects that their health information may be used in research and allowing them an opportunity to object to the use of their information. [Fn 43]

Comparing state statutes to the final rule: The variability of state law regarding privacy of individually identifiable health information and the limitations of the applicability of many such laws demonstrates the need for uniformity and minimum standards for privacy protection. This regulation is designed to meet these goals while allowing stricter state laws to be enacted and remain effective. A comparison of state privacy laws with the final regulation highlights several of the rule's key implications:

- No state law requires covered entities to make their privacy and access policies available to patients. Thus, all covered entities that have direct contact with patients will be required by this rule to prepare a statement of their privacy protection and access policies. This necessarily assumes that entities have to develop procedures if they do not already have them in place.
- The rule will affect more entities than are covered or encompassed under many state laws.
- Among the three categories of covered entities, it appears that health plans will be the most significantly affected by the access provisions of the rule. Based on the Health Insurance Association of America (HIAA) data [fn 44], there are approximately 94.7 million non-elderly persons with private health insurance in the 35 states that do not provide patients a legal right to inspect and copy their records.
- Under the rule, covered entities will have to obtain an individual's authorization before they could use or disclose their information for purposes other than treatment, payment, and health care operations—except in the situations explicitly defined as allowable disclosures without authorization. Although the final rule would establish a generally uniform disclosure and re-disclosure requirement for all covered entities, the entities that currently have the greatest ability and economic incentives to use and disclose protected health information for marketing services to both patients and health care providers without individual authorization.
- While the final rule appears to encompass many of the requirements found in current state laws, it also is clear that within state laws, there are many

1/3/2003

provisions that cover specific cases and health conditions. Certainly, in states that have no restrictions on disclosure, the rule will establish a baseline standard. But in states that do place conditions on the disclosure of protected health information, the rule may place additional requirements on covered entities.

3. Other Federal Laws

The relationship with other federal statutes is discussed above in the preamble.

...

V. Final Regulatory Flexibility Analysis

No preemption information.

VI. Unfunded Mandates

No preemption information.

VII. Environmental Impact

No preemption information.

VIII. Collection of Information Requirements

Section 160.204—Process for Requesting Exception Determinations

Section 160.204 would require persons requesting to except a provision of state law from preemption under § 160.203(a) to submit a written request, that meets the requirements of this section, to the Secretary to except a provision of state law from preemption under § 160.203. The burden associated with these requirements is the time and effort necessary for a state to prepare and submit the written request for an exception determination to the Secretary for approval. On an annual basis it is estimated that it will take 40 states 16 hours each to prepare and submit a request. The total annual burden associated with this requirement is 640 hours. The Department solicits public comment on the number of requests and hours for others likely to submit requests. [82794 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations]

1/3/2003

IX. Executive Order 13132: Federalism

The Department has examined the effects of provisions in the final privacy regulation on the relationship between the federal government and the states, as required by Executive Order 13132 on "Federalism." Our conclusion is that the final rule does have federalism implications because the rule has substantial direct effects on states, on the relationship between the national government and states, and on the distribution of power and responsibilities among the various levels of government. The federalism implications of the rule, however, flow from, and are consistent with the underlying statute. The statute allows us to preempt state or local rules that provide less stringent privacy protection requirements than federal law is consistent with this Executive Order. Overall, the final rule attempts to balance both the autonomy of the states with the necessity to create a federal benchmark to preserve the privacy of personally identifiable health information. It is recognized that the states generally have laws that relate to the privacy of individually identifiable health information. The HIPAA statute dictates the relationship between state law and this final rule. Except for laws that are specifically exempted by the HIPAA statute, state laws continue to be enforceable, unless they are contrary to Part C of Title XI of the standards, requirements, or implementation specifications adopted or pursuant to subpart x. However, under section 264(c)(2), not all contrary provisions of state privacy laws are preempted; rather, the law provides that contrary provisions of state law relating to the privacy of individually identifiable health information that are also "more stringent" than the federal regulatory requirements or implementations specifications will continue to be enforceable. Section 3(b) of Executive Order 13132 recognizes that national action limiting the policymaking discretion of states will be imposed " * * * only where there is constitutional and statutory authority for the action and the national activity is appropriate in light of the presence of a problem of national significance." Personal privacy issues are widely identified as a national concern by virtue of the scope of interstate health commerce. HIPAA's provisions reflect this position. HIPAA attempts to facilitate the electronic exchange of financial and administrative health plan transactions while recognizing challenges that local, national, and international information sharing raise to confidentiality and privacy of health information. agency's goal of ensuring that all patients who receive medical services are assured a minimum level of personal privacy. Particularly where the absence of privacy protection undermines an individual's access to health care services, both the personal and public interest is served by establishing federal rules.

Section 3(d)(2) of the Executive Order 13132 requires the federal government defer to the states to establish standards where possible. HIPAA requires the Department to establish standards, and we have done so accordingly. This approach is a key component of the final Privacy Rule, and it adheres to section 4(a) of Executive Order 13132, which expressly contemplates preemption when there is a conflict between exercising state and federal authority under federal statute. Section 262 of HIPAA enacted Section 1178 of the Social Security Act, developing a "general rule"

1/3/2003

that state laws or provisions that are contrary to the provisions or requirements of Part C of Title XI, or the standards or implementation specifications adopted, or established thereunder are preempted. Several exceptions to this rule exist, each of which is designed to maintain a high degree of state autonomy. Moreover, section 4(b) of the Executive Order authorizes preemption of state law in the federal rule making context when there is “the exercise of state authority is directly conflicts with the exercise of federal authority under federal statute * * *.” Section 1178 (a)(2)(B) of HIPAA specifically preempts state laws related to the privacy of individually identifiable health information unless the state law is more stringent. Thus, we have interpreted state and local laws and regulations that would impose less stringent requirements for protection of individually identifiable health information as undermining the agency’s goal of ensuring that all patients who receive medical services are assured a minimum level of personal privacy. Particularly where the absence of privacy protection undermines an individual’s access to health care services, both the personal and public interest is served by establishing federal rules. The final rule would establish national minimum standards with respect to the collection, maintenance, access, use, and disclosure of individually identifiable health information. The federal law will preempt state law only where state and federal laws are “contradictory” and the federal regulation is judged to establish “more stringent” privacy protections than state laws. As required by the previous Executive Order (E.O. 13132), states and local governments were given, through the notice of proposed rule making, an opportunity to participate in the proceedings to preempt state and local laws (section 4(e)). The Secretary also provided a review of preemption issues upon requests from states. In addition, anticipating the promulgation of the Executive Order, appropriate officials and organizations were consulted before this proposed action is implemented (Section 3(a) of Executive Order 13132). The same section also includes some qualitative discussion of costs that would occur beyond that time period. Most of the costs of proposed rule, however, would occur in the years immediately after the publication of a final rule. Future costs beyond the ten year period will continue but will not be as great as the initial compliance costs. Finally, we have considered the cost burden that this proposed rule would impose on state and local health care programs, such as Medicaid, county hospitals, and other state health benefits programs. As discussed in Section E of the Regulatory Impact Analysis of this document, we estimate state and local government costs will be in the order of \$460 million in 2003 and \$2.4 billion over ten years. The agency concludes that the policy in this final document has been assessed in light of the principles, criteria, and requirements in Executive Order 13132; that this policy is not inconsistent with that Order; that this policy will not impose significant additional costs and burdens on the states; and that this policy will not affect the ability of the states to discharge traditional state governmental functions. During our consultation with the states, representatives from various state agencies and offices expressed concern that the final regulation would preempt [82797 Federal Register / Vol. 65, No. 250 / Thursday, December 28, 2000 / Rules and Regulations] all state privacy laws. As explained in this section, the regulation

1/3/2003

would only preempt state laws where there is a direct conflict between state laws and the regulation, and where the regulation provides more stringent privacy protection than state law. We discussed this issue during our consultation with state representatives, who generally accepted our approach to the preemption issue. During the consultation, we requested further information from the states about whether they currently have laws requiring that providers have a “duty to warn” family members or third parties about a patient’s condition other than in emergency circumstances. Since the consultation, we have not received additional comments or questions from the states.

X. Executive Order 13086: Consultation and Coordination With Indian Tribal Governments

No preemption information.

TITLE 45--PUBLIC WELFARE

SUBTITLE A--DEPARTMENT OF HEALTH
AND HUMAN SERVICES

PART 160--GENERAL ADMINISTRATIVE REQUIREMENTS--Table of Contents

Subpart B--Preemption of State Law

Sec. 160.201 Applicability.

The provisions of this subpart implement section 1178 of the Act, as added by section 262 of Public Law 104-191.

Sec. 160.202 Definitions.

For purposes of this subpart, the following terms have the following meanings:

Contrary, when used to compare a provision of State law to a standard, requirement, or implementation specification adopted under this subchapter, means:

- (1) A covered entity would find it impossible to comply with both the State and federal requirements; or
- (2) The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of part

1/3/2003

C of title XI of the Act or section 264 of Pub. L. 104-191, as applicable.

More stringent means, in the context of a comparison of a provision of State law and a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter, a State law that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under this subchapter, except if the disclosure is:

(i) Required by the Secretary in connection with determining whether a covered entity is in compliance with this subchapter; or

(ii) To the individual who is the subject of the individually identifiable health information.

(2) With respect to the rights of an individual who is the subject of the individually identifiable health information of access to or amendment of individually identifiable health information, permits greater rights of access or amendment, as applicable; provided that, nothing in this subchapter may be construed to preempt any State law to the extent that it authorizes or prohibits disclosure of protected health information about a minor to a parent, guardian, or person acting in loco parentis of such minor.

(3) With respect to information to be provided to an individual who is the subject of the individually identifiable health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form or substance of an authorization or consent for use or disclosure of individually identifiable health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the authorization or consent, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individually identifiable health information.

Relates to the privacy of individually identifiable health information means, with respect to a State law, that the State law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

State law means a constitution, statute, regulation, rule, common

1/3/2003

law, or other State action having the force and effect of law.

Sec. 160.203 General rule and exceptions.

A standard, requirement, or implementation specification adopted under this subchapter that is contrary to a provision of State law preempts the provision of State law. This general rule applies, except if one or more of the following conditions is met:

(a) A determination is made by the Secretary under Sec. 160.204 that the provision of State law:

(1) Is necessary:

(i) To prevent fraud and abuse related to the provision of or payment for health care;

(ii) To ensure appropriate State regulation of insurance and health plans to [[Page 672]] the extent expressly authorized by statute or regulation;

(iii) For State reporting on health care delivery or costs; or

(iv) For purposes of serving a compelling need related to public health, safety, or welfare, and, if a standard, requirement, or implementation specification under part 164 of this subchapter is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or

(2) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

(b) The provision of State law relates to the privacy of health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter.

(c) The provision of State law, including State procedures established under such law, as applicable, provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention.

(d) The provision of State law requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

Sec. 160.204 Process for requesting exception determinations.

(a) A request to except a provision of State law from preemption under Sec. 160.203(a) may be submitted to the Secretary. A request by a State must be submitted through its chief elected official, or his or

1/3/2003

her designee. The request must be in writing and include the following information:

- (1) The State law for which the exception is requested;
 - (2) The particular standard, requirement, or implementation specification for which the exception is requested;
 - (3) The part of the standard or other provision that will not be implemented based on the exception or the additional data to be collected based on the exception, as appropriate;
 - (4) How health care providers, health plans, and other entities would be affected by the exception;
 - (5) The reasons why the State law should not be preempted by the federal standard, requirement, or implementation specification, including how the State law meets one or more of the criteria at Sec. 160.203(a); and
 - (6) Any other information the Secretary may request in order to make the determination.
- (b) Requests for exception under this section must be submitted to the Secretary at an address that will be published in the Federal Register. Until the Secretary's determination is made, the standard, requirement, or implementation specification under this subchapter remains in effect.
- (c) The Secretary's determination under this section will be made on the basis of the extent to which the information provided and other factors demonstrate that one or more of the criteria at Sec. 160.203(a) has been met.

1/3/2003